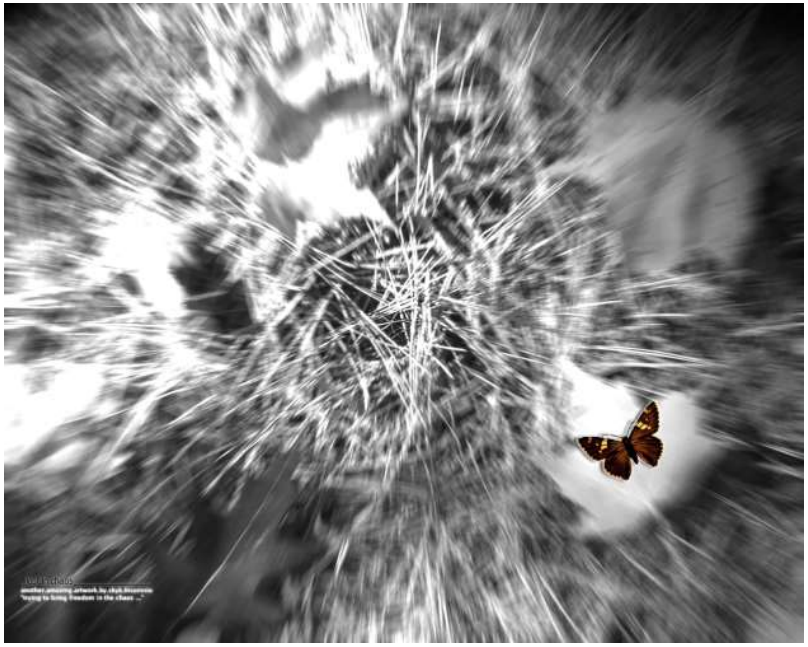
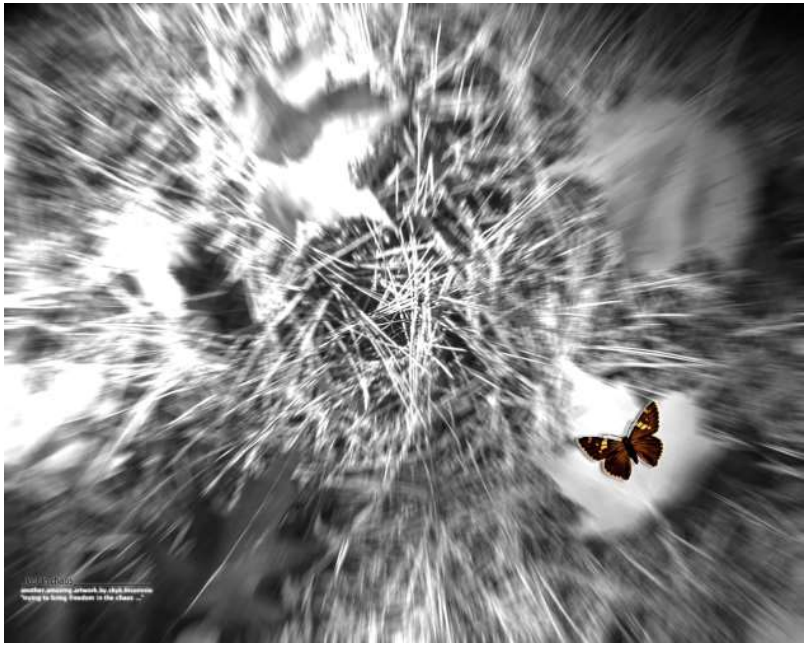


Robert Garigue

VP and Chief Information Security Officer

Controlling Order and Disorder

The evolving role of the CISO within the new structures of Information Systems



Robert Garigue

VP and Chief Information Security Officer

Controlling Order and Disorder

The evolving role of the CISO within the new structures of Information Systems

Outline of our expedition

Background and Analysis Frameworks
- Business models
- The nature of the threats

The strategic information security framework
- Environmental factors
- Information security processes

Evolution of information security functions
- Alignment and Integration challenges
- Emerging new risks and concerns

Reflections on the nature and evolving role of the Chief Information Security Officer

BMO Financial Group

- Founded in 1817 – First Canadian Bank
- Highly diversified financial institution
  - retail banking
  - wealth management
  - investment banking
- Assets of $256 billion at October 31, 2003
- 34,000 employees
- Strong presence in US Mid-West through Harris Bankcorp
- Overseas offices around the world

Metrics of the Digital BMO

200+ Mainframes

276+ Open System Business Critical Applications

37 000 Desktops

2500 support servers

6000 main network devices

165 Terabytes of data
storage 50%+ a year

Several Million Transactions/sec

Myths and Realities

For some the world is a multidimensional place

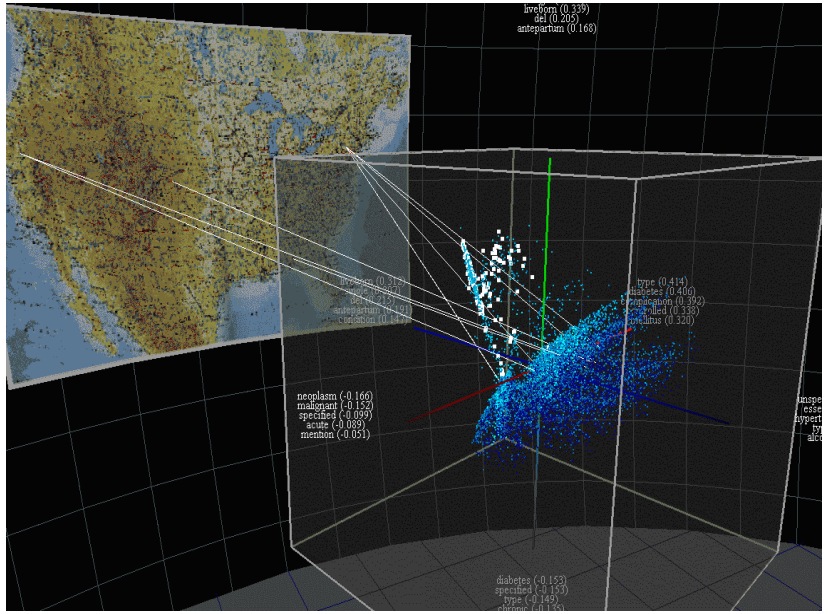
…and for other… it is still flat…

There are always Myths and Realities.

An evolving organizational context : Information Society

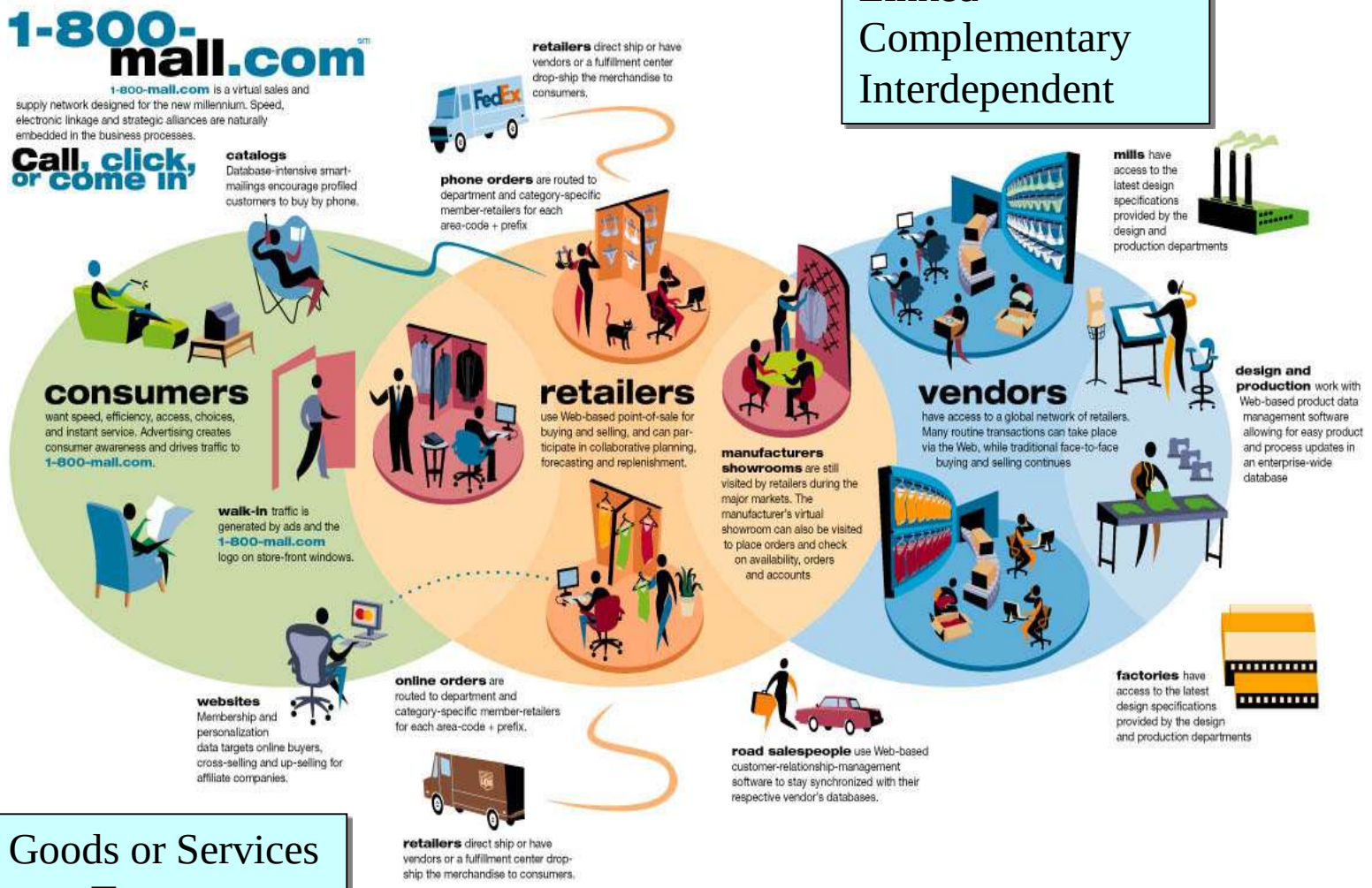
Some of the New Realities:

- Information based productivity
- Computer mediated decisions
- Rise of the knowledge worker
- Network centric structures and value chains
- Command and Control hierarchies are displaced by Cooperative, Commutative and Coordinated organizations
- “a burden shared is a burden halved .. an intellectual asset shared is one doubled”



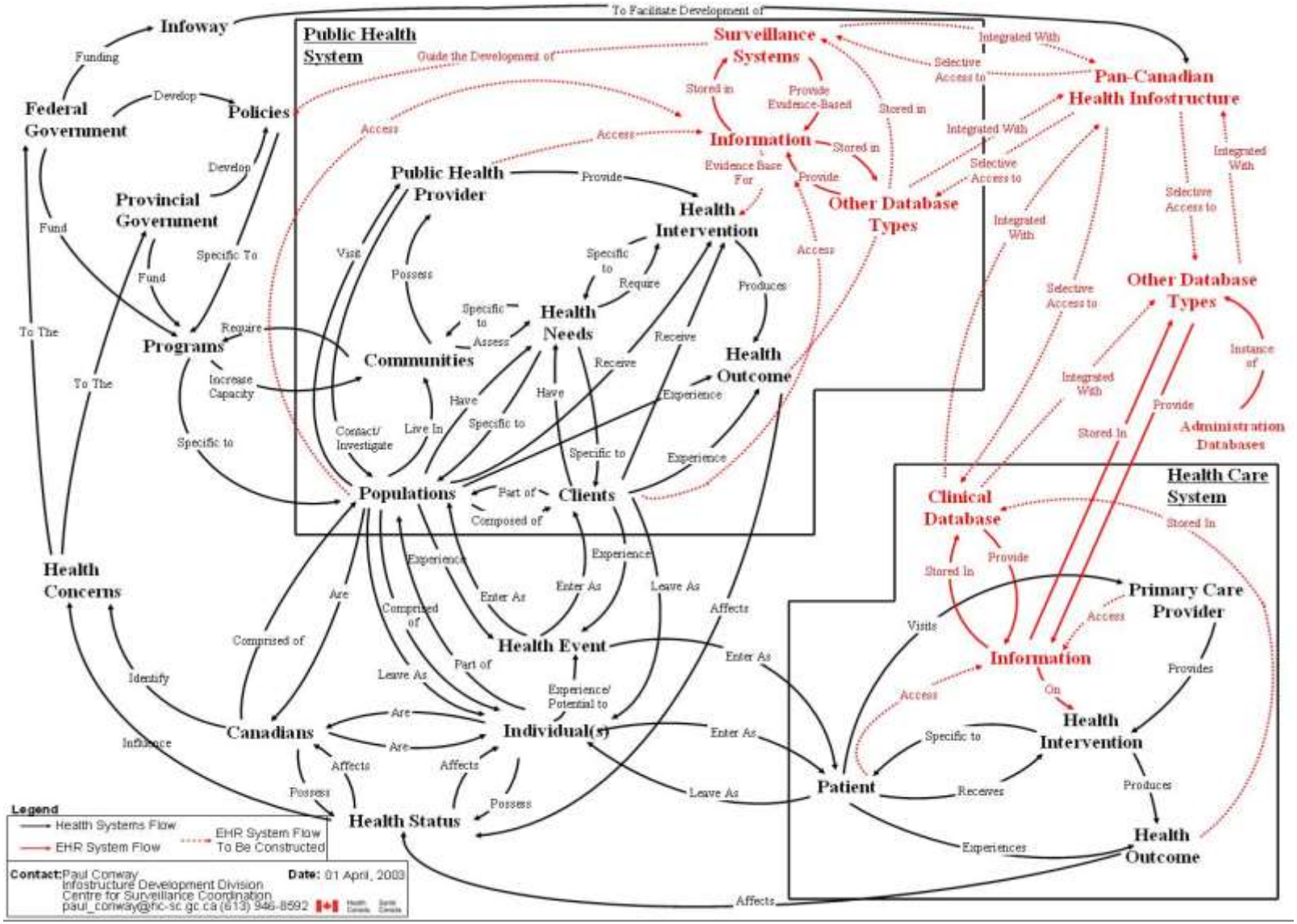
The Integrated Informational Value-Chain

Linked
Complementary
Interdependent

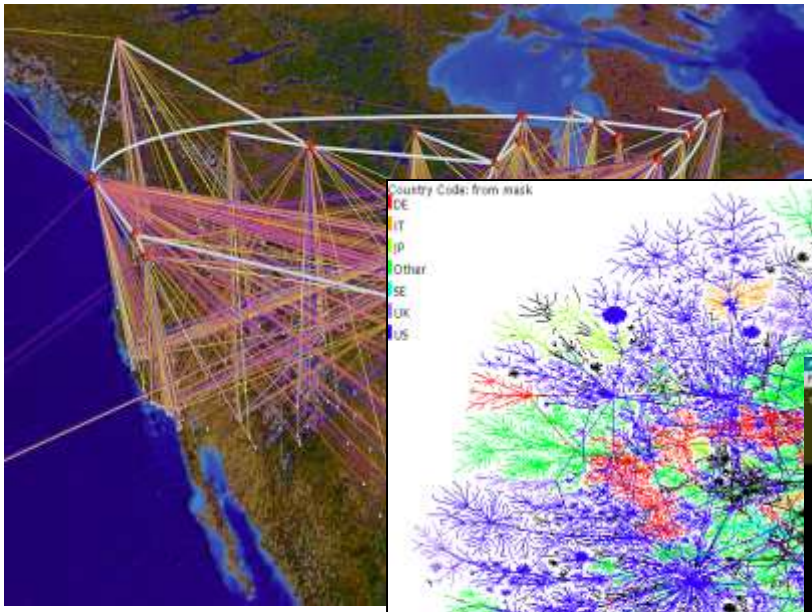

1-800-mall.com
1-800-mall.com is a virtual sales and supply network designed for the new millennium. Speed, electronic linkage and strategic alliances are naturally embedded in the business processes.
Call, click, or come in
catalogs
Database-intensive smart-mailings encourage profiled customers to buy by phone.
retailers direct ship or have vendors or a fulfillment center drop-ship the merchandise to consumers.
FedEx
phone orders are routed to department and category-specific member-retailers for each area-code + prefix
consumers
want speed, efficiency, access, choices, and instant service. Advertising creates consumer awareness and drives traffic to 1-800-mall.com.
walk-in traffic is generated by ads and the 1-800-mall.com logo on store-front windows.
retailers
use Web-based point-of-sale for buying and selling, and can participate in collaborative planning, forecasting and replenishment.
manufacturers showrooms are still visited by retailers during the major markets. The manufacturer's virtual showroom can also be visited to place orders and check on availability, orders and accounts
vendors
have access to a global network of retailers. Many routine transactions can take place via the Web, while traditional face-to-face buying and selling continues
mills have access to the latest design specifications provided by the design and production departments
design and production work with Web-based product data management software allowing for easy product and process updates in an enterprise-wide database
factories have access to the latest design specifications provided by the design and production departments
websites
Membership and personalization data targets online buyers, cross-selling and up-selling for affiliate companies.
online orders are routed to department and category-specific member-retailers for each area-code + prefix.
road salespeople use Web-based customer-relationship-management software to stay synchronized with their respective vendor's databases.
retailers direct ship or have vendors or a fulfillment center drop-ship the merchandise to consumers.

From Goods or Services
To
Goods with Services

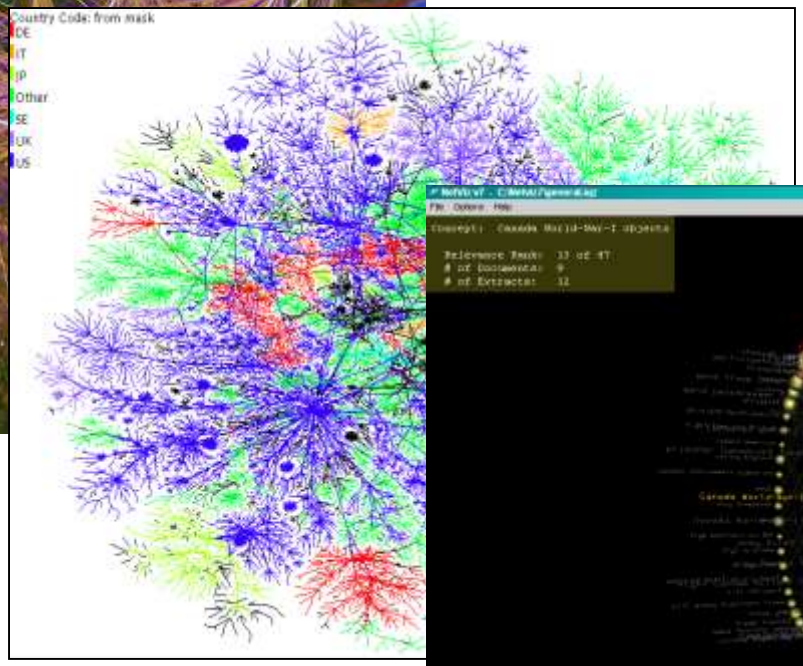
Information Flows : Health Care Ecosystem



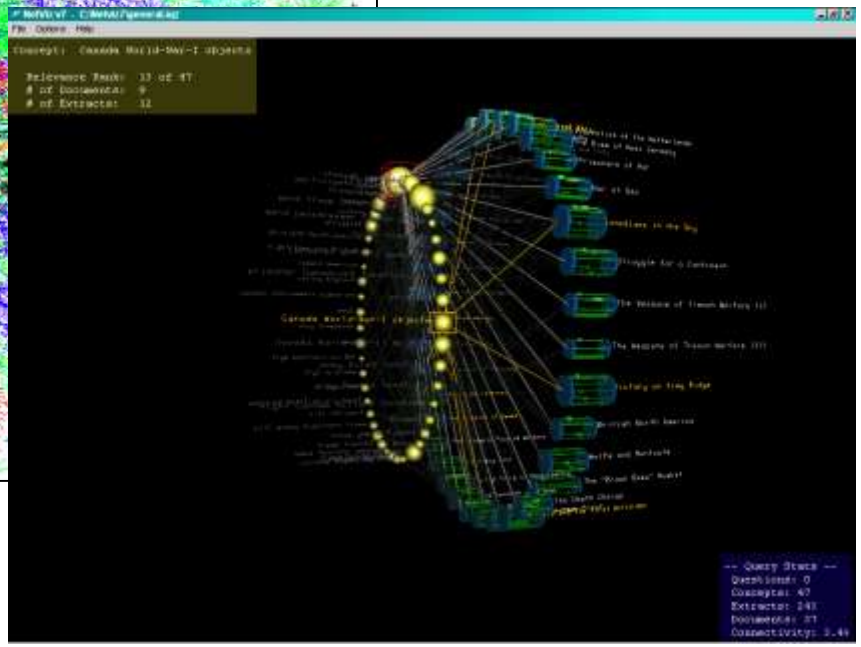
The impact will be felt in the three realms of cyberspace



Physical

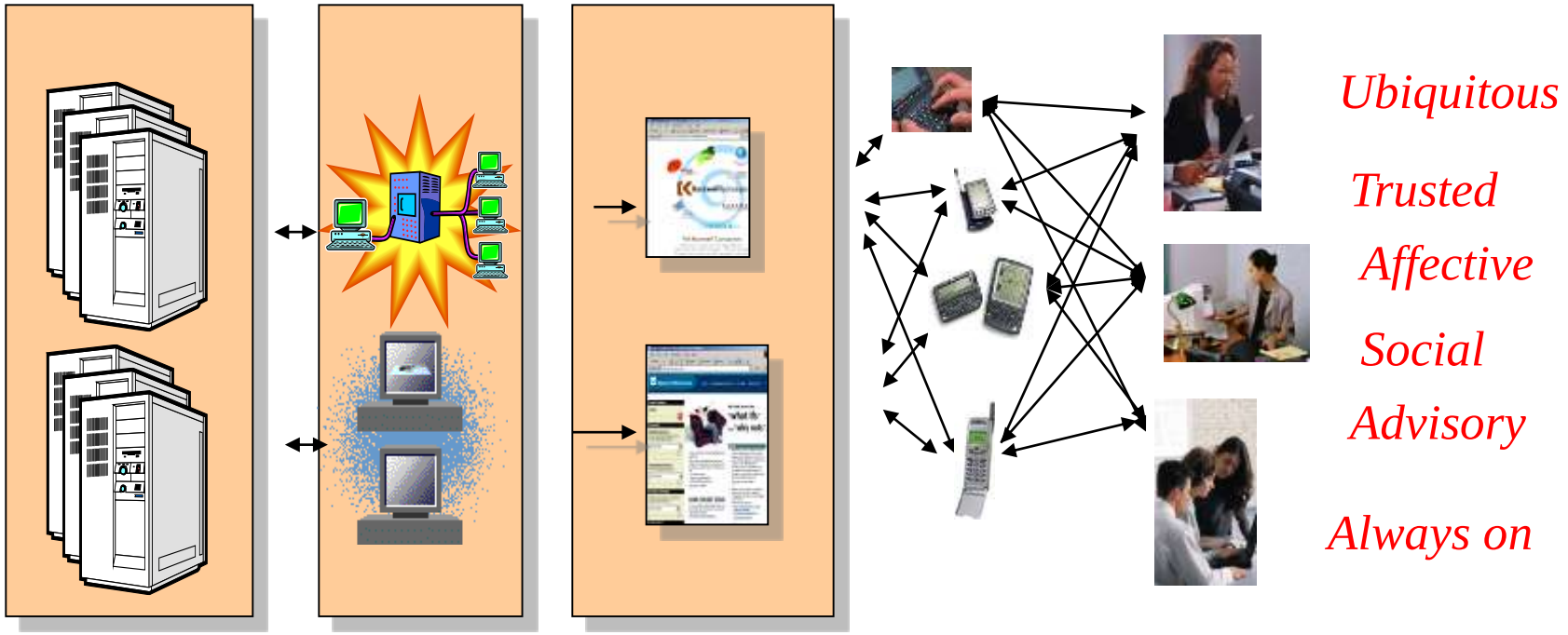


Process



Content

The Evolution of the Noosphere (Teilhard de Chardin)



Organizations
(command and control)

focus

Individuals
(cooperation, coordination,
and communication)

It is full of Risk: These are the shape of "Things Now Dead"

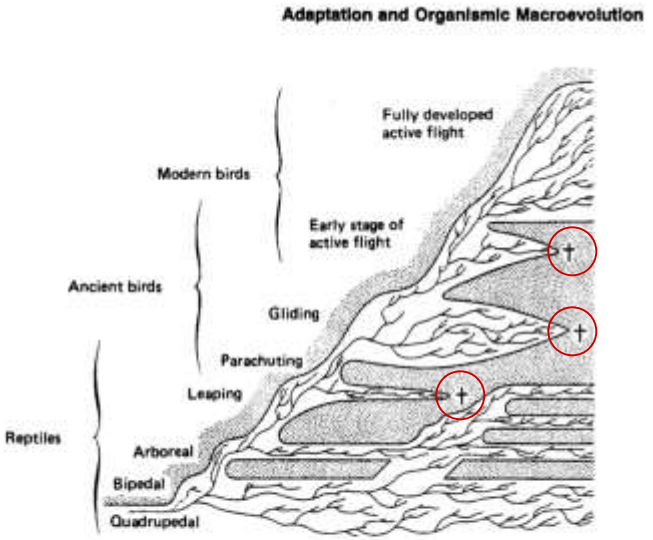
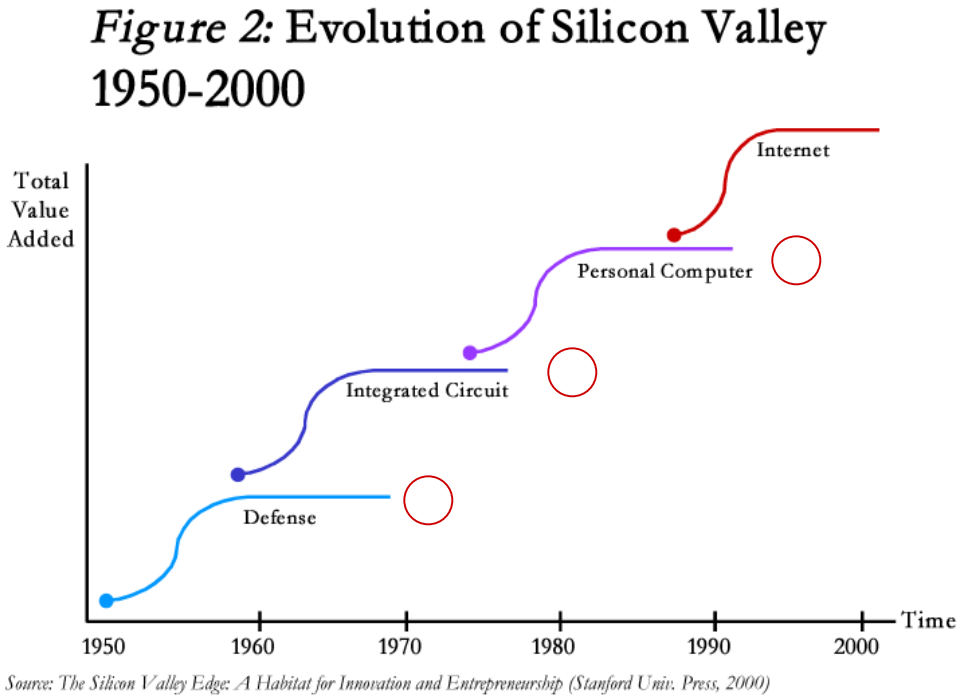


Figure 2.6 Bock's "schematic model showing the different stages in the evolution of birds through successive taxonomic groups—reptiles, ancient birds, and modern birds. The possibilities of transitional zones appearing several times and of their continued existence, for example, at the arboreal and leaping levels, are emphasized in this model. Moreover, the model illustrates the severe selection pressure exerted by flying birds on other arboreal groups that may be evolving fully developed aerial adaptations." (Redrawn from Bock, 1979, Fig. 16, p. 54)



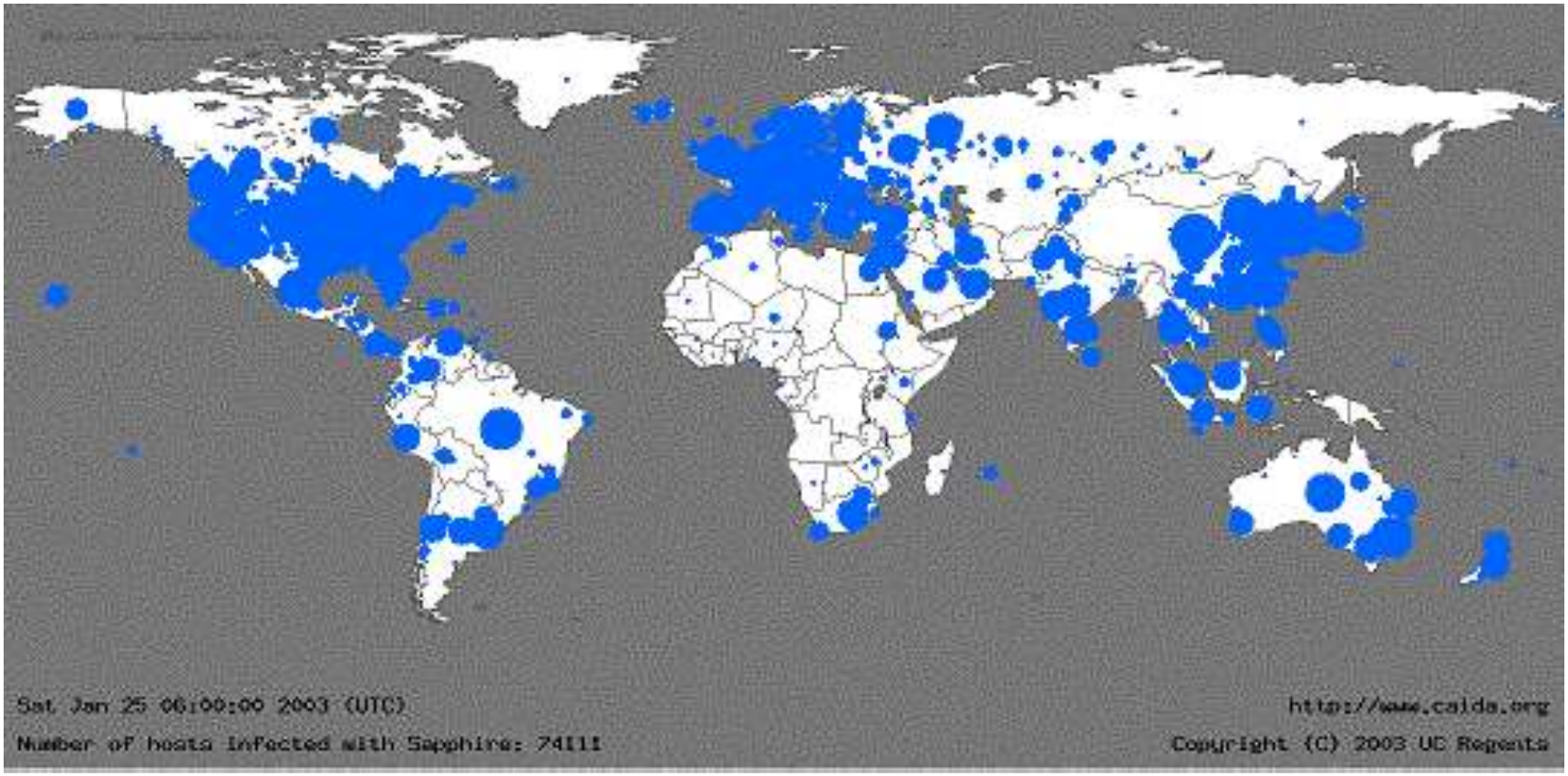
Source: The Silicon Valley Edge: A Habitat for Innovation and Entrepreneurship (Stanford Univ. Press, 2000)

But there will always be conflict between Open systems and Closed systems…. Violent conflict …

Pablo Picasso. ***Guernica.*** 1937. Oil on canvas. Museo del Prado, Madrid, Spain

Experts fear cyberspace could be terrorists' next target
USA, world's most wired nation, has much to lose
By Jon Swartz
USA TODAY
Cyberwarfare scenarios
In a nation tightly wired to the Internet, the notion of cyberterrorism — using the World Wide Web to electronically attack the USA — is being given a higher priority since Sept. 11 terrorist attacks in New York and Washington. Some of the ways cyberterrorists could wreak havoc in the USA:
Very Likely
► Denial-of-service attacks.
► Computer worms and viruses.
Likely
► Hackers breaking into government computers and stealing military secrets and encryption technology.
► Power grid disruption.
► Emergency systems compromised, complicating rescue efforts in tandem with bombing of symbolic buildings.
Unlikely
► Cutting of fiber-optic cables between major hubs.
► Bombing or physically attacking domain-name servers or switching banks.
Unlikely
► Bombing of Internet facilities to take down the Internet.

Zero-day virus
Slammer – 30 minutes later



Information Security: A new oxymoron

Information

Security

The debate

Arguments For Getting Funding : Levels of Maturity of the Organization

Fear, Uncertainty and Despair:
"The Hackers, virus, will get us unless.."

The Heard Mentality:
"The king needs Taxes"…

The Analytical ROI ?
"Investment in Intrusion Prevention Systems are better than"…

Arguments that have yet to come:

"Because we can take on more business and manage more risks"

(brakes enable cars can go faster)

Information Security – Managing Expectations
Sometimes it is just a communication issue…

Consequence A: Information Security Officer as The Jester

Sees a lot

Can tell the king he has no clothes

Can tell the king he really is ugly

Does not get killed by the king

Nice to have around but…how much security improvement comes from this ?

Consequence B: Information Security Officer as Road Kill

Changes happened faster that he was able to move

Did not read the signs

Good intentions went unfulfilled

A brutal way to ending a promising career

Sad to have around but…how much security improvement comes from this ?

Maybe a better model for CISO: Charlemagne

- King of the Franks and Holy Roman Emperor; conqueror of the Lombards and Saxons (742-814) - reunited much of Europe after the Dark Ages.

- He set up other schools, opening them to peasant boys as well as nobles. Charlemagne never stopped studying. He brought an English monk, Alcuin, and other scholars to his court - encouraging the development of a standard script.

- He set up money standards to encourage commerce, tried to build a Rhine-Danube canal, and urged better farming methods. He especially worked to spread education and Christianity in every class of people.

- He relied on **Counts**, **Margraves** and **Missi Domini** to help him.

Margraves - Guard the frontier districts of the empire. Margraves retained, within their own jurisdictions, the authority of dukes in the feudal arm of the empire.

Missi Domini - Messengers of the King.

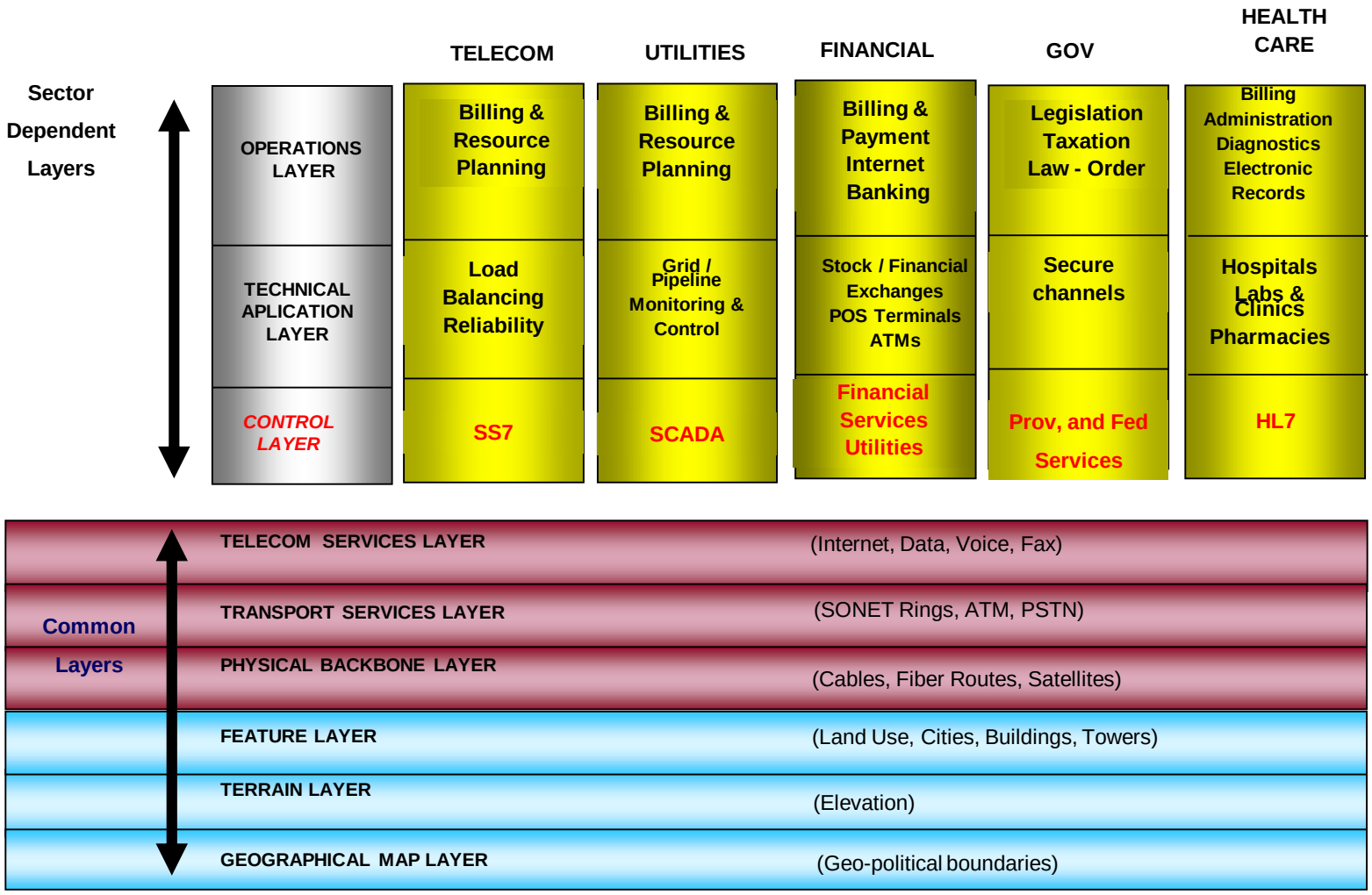
Knowledge of “risky things” is of strategic value

How to know today tomorrow’s unknown ?

How to structure information security processes in an organization so as to identify and address the NEXT categories of risks ?

This is the mandate of information security.

The Interconnected Societies: the critical Infrastructure



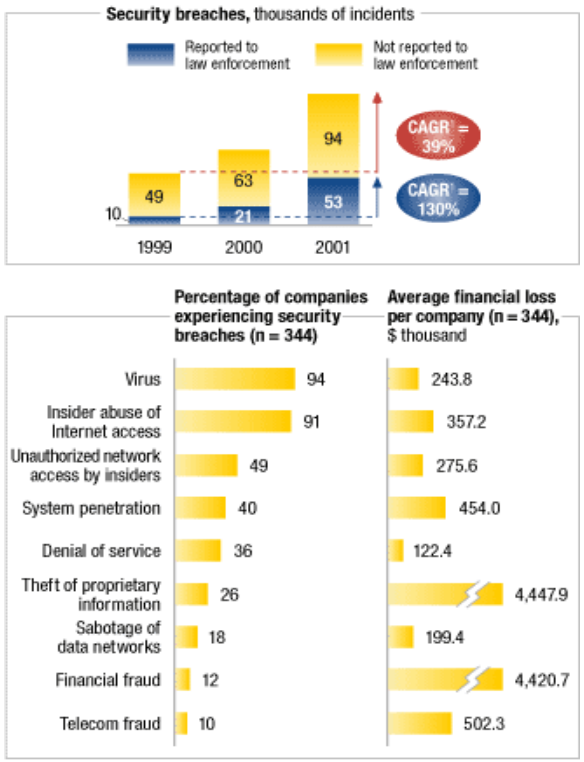
Indicators and warnings
External environment : the rates of evolutions

- 16 new malware products launched every day: viruses, worms, trojan horses, spyware etc
- 7 new vulnerabilities discovered every day
- 20 minutes guaranty
- Probes against Financial Institutions web sites launched every 6 seconds
- Social engineering is on the rise: People are the weak link

Indicators and warnings : Threats and targets

EXHIBIT 1

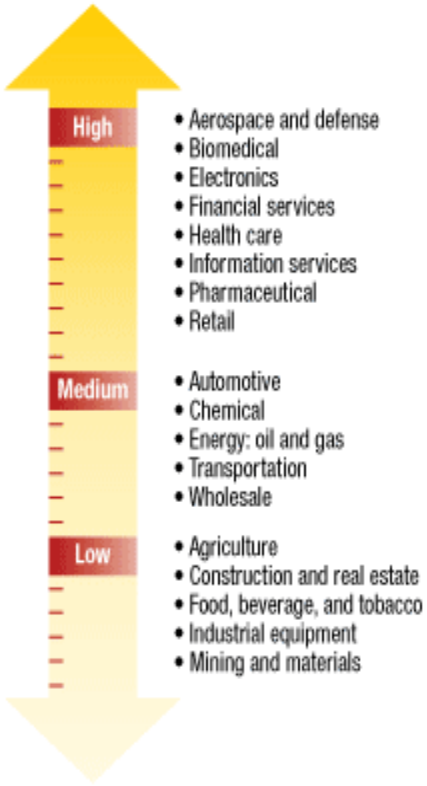
Hackers, viruses, and worms

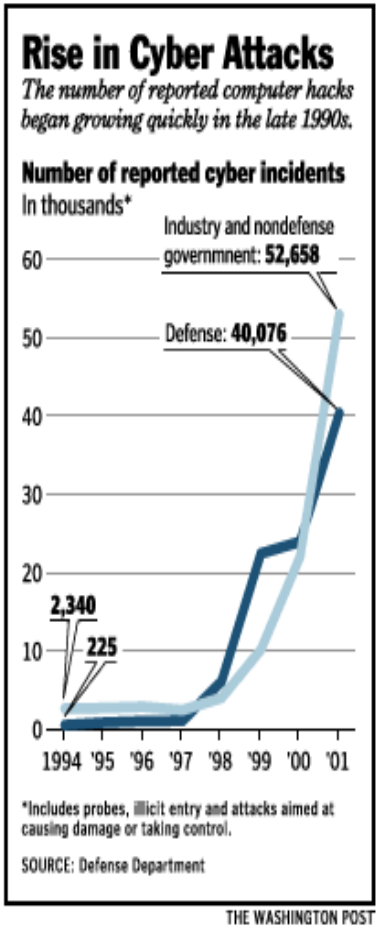


[1]Compound annual growth rate.
Source: *Computerworld*, January 2002; CSI/FBI Computer Crime and Security Survey, 2001

EXHIBIT 2

Variable degrees of risk

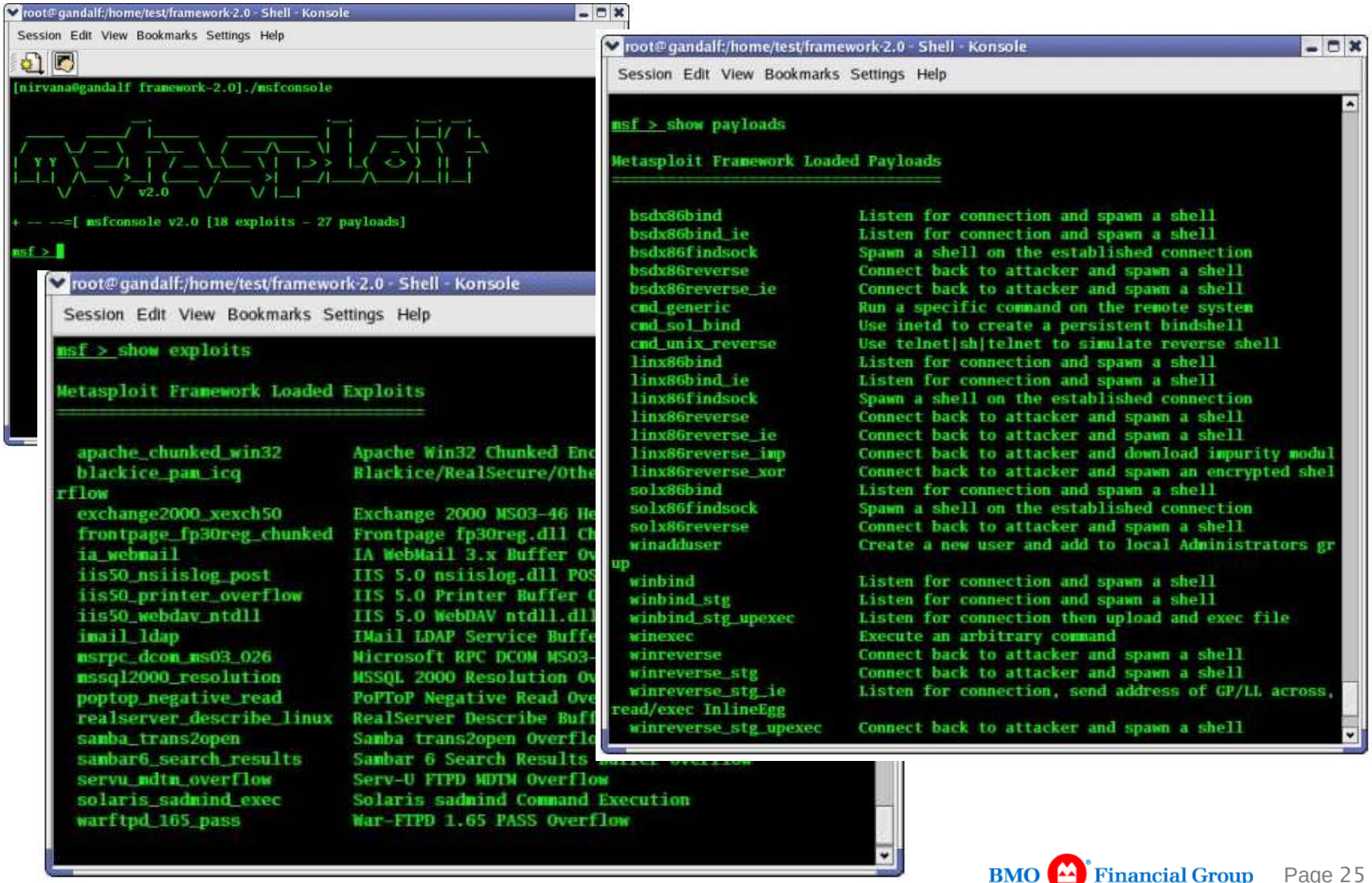




THE WASHINGTON POST

The McKinsey Quarterly, 2002 Number 2 Risk and resilience
Daniel F. Lohmeyer, Jim McCrory, and Sofya Pogreb

Manufacturing exploits: The electronic Petrie Dish
Malware : spyware + trojan + spam + exploits + social engineering


root@gandalf:/home/test/framework-2.0 - Shell - Konsole
Session Edit View Bookmarks Settings Help
[nirvana@gandalf framework-2.0]./msfconsole
v2.0
+ -- --=[msfconsole v2.0 [18 exploits - 27 payloads]
msf >
root@gandalf:/home/test/framework-2.0 - Shell - Konsole
Session Edit View Bookmarks Settings Help
msf > show exploits
Metasploit Framework Loaded Exploits
apache_chunked_win32 Apache Win32 Chunked Enc
blackice_pam_icq Blackice/RealSecure/Othe
rflow
exchange2000_xexch50 Exchange 2000 MS03-46 He
frontpage_fp30reg_chunked Frontpage fp30reg.dll Ch
ia_webmail IA WebMail 3.x Buffer Ov
iis50_nsiislog_post IIS 5.0 nsiislog.dll POS
iis50_printer_overflow IIS 5.0 Printer Buffer O
iis50_webdav_ntdll IIS 5.0 WebDAV ntdll.dll
imail_ldap IMail LDAP Service Buffe
msrpc_dcom_ms03_026 Microsoft RPC DCOM MS03-
mssql2000_resolution MSSQL 2000 Resolution Ov
poptop_negative_read PoPToP Negative Read Ove
realserver_describe_linux RealServer Describe Buff
samba_trans2open Samba trans2open Overflo
sambar6_search_results Sambar 6 Search Results
servu_mdtm_overflow Serv-U FTPD MDTM Overflow
solaris_sadmind_exec Solaris sadmind Command Execution
warftpd_165_pass War-FTPD 1.65 PASS Overflow
root@gandalf:/home/test/framework-2.0 - Shell - Konsole
Session Edit View Bookmarks Settings Help
msf > show payloads
Metasploit Framework Loaded Payloads
bsdx86bind Listen for connection and spawn a shell
bsdx86bind_ie Listen for connection and spawn a shell
bsdx86findsock Spawn a shell on the established connection
bsdx86reverse Connect back to attacker and spawn a shell
bsdx86reverse_ie Connect back to attacker and spawn a shell
cmd_generic Run a specific command on the remote system
cmd_sol_bind Use inetd to create a persistent bindshell
cmd_unix_reverse Use telnet|sh|telnet to simulate reverse shell
linx86bind Listen for connection and spawn a shell
linx86bind_ie Listen for connection and spawn a shell
linx86findsock Spawn a shell on the established connection
linx86reverse Connect back to attacker and spawn a shell
linx86reverse_ie Connect back to attacker and spawn a shell
linx86reverse_imp Connect back to attacker and download impurity modul
linx86reverse_xor Connect back to attacker and spawn an encrypted shel
solx86bind Listen for connection and spawn a shell
solx86findsock Spawn a shell on the established connection
solx86reverse Connect back to attacker and spawn a shell
winadduser Create a new user and add to local Administrators gr
up
winbind Listen for connection and spawn a shell
winbind_stg Listen for connection and spawn a shell
winbind_stg_upexec Listen for connection then upload and exec file
winexec Execute an arbitrary command
winreverse Connect back to attacker and spawn a shell
winreverse_stg Connect back to attacker and spawn a shell
winreverse_stg_ie Listen for connection, send address of GP/LL across,
read/exec InlineEgg
winreverse_stg_upexec Connect back to attacker and spawn a shell

Indicators and warnings
How money was lost – Rough order of magnitude (ROM)

	Highest Reported '000 US$	Average losses '000 US$
Denial of Service	60,000	1,427
Theft of proprietary information	35,000	2,700
Insider abuse of Net access	6,000	135
Viruses and worms	6,000	200
Financial fraud involving info. systems	4,000	329
Sabotage of data or networks	2,000	215
Laptop theft	2,000	47
System penetration by outsider (hacking)	1,000	56
Active wiretapping	700	352
Telecom fraud	250	50
Unauthorized insider access	100	31
Telecom eavesdropping	50	15

Source: CFI/FBI Report 2003
530 US based corporations, government and educ. inst.

Identity Theft in Canada

Home • Search • Contact Us • Français
PHONEBUSTERS

2003		
PROVINCES	VICTIMS	$ LOSS
ON	5772	$12,682,218.64
BC	1829	$1,808,318.45
AB	1079	$1,282,716.71
MB	195	$194,718.93
SK	202	$687,992.85
UNKNOWN	34	$5,640.02
NB	200	$261,206.11
NS	223	$273,347.29
NF	94	$115,993.06
PE	14	$2,150.00
NT	2	$0
QC	3711	$4,246,801.90
YT	2	$0
NU	2	$3000
TOTALS	13359	$21,564,103.96

2002		
PROVINCES	VICTIMS	$ LOSS
ON	4031	$7,188,125.90
BC	1046	$1,221,733.15
AB	635	$767,110.16
MB	196	$187,843.92
SK	106	$84,937.37
UNKNOWN	144	$12,885.00
NB	131	$150,016.54
NS	185	$222,516.14
NF	46	$27,480.20
PE	16	$7,083.42
NT	2	$0
QC	1646	$1,916,011.64
YT	2	$0
NU	1	$1,100.00
TOTALS	8187	$11,786,843.44

Hacking Beliefs

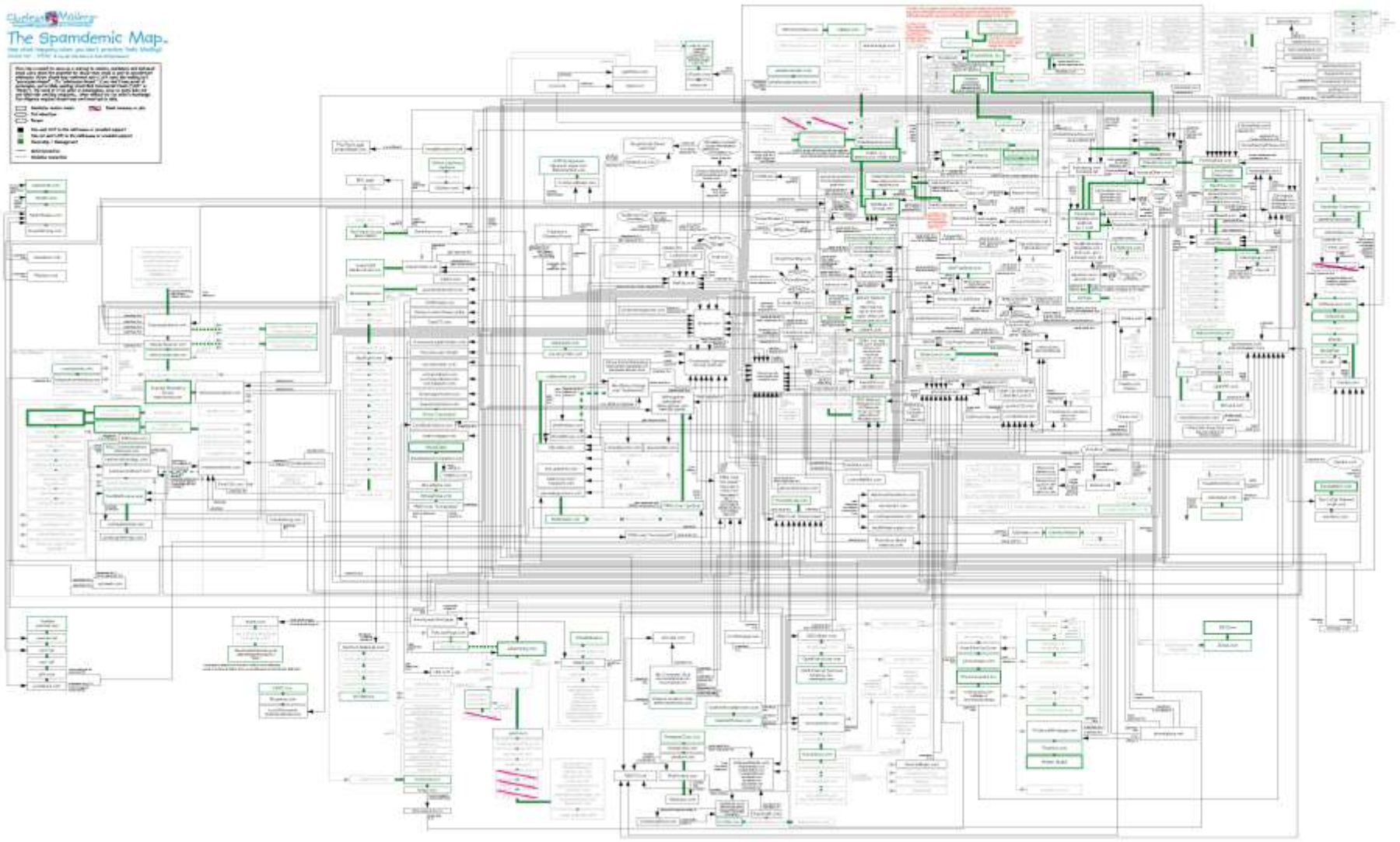
Identity Theft

- One of the fastest growing crimes. Statistics Canada reports 13,359 cases, $21.5 million losses in 2003
- Account takeover (credit cards, bank accounts)
- Application fraud (open new accounts with victim's ID)
- Industry needs improved identity management solutions and strong public awareness

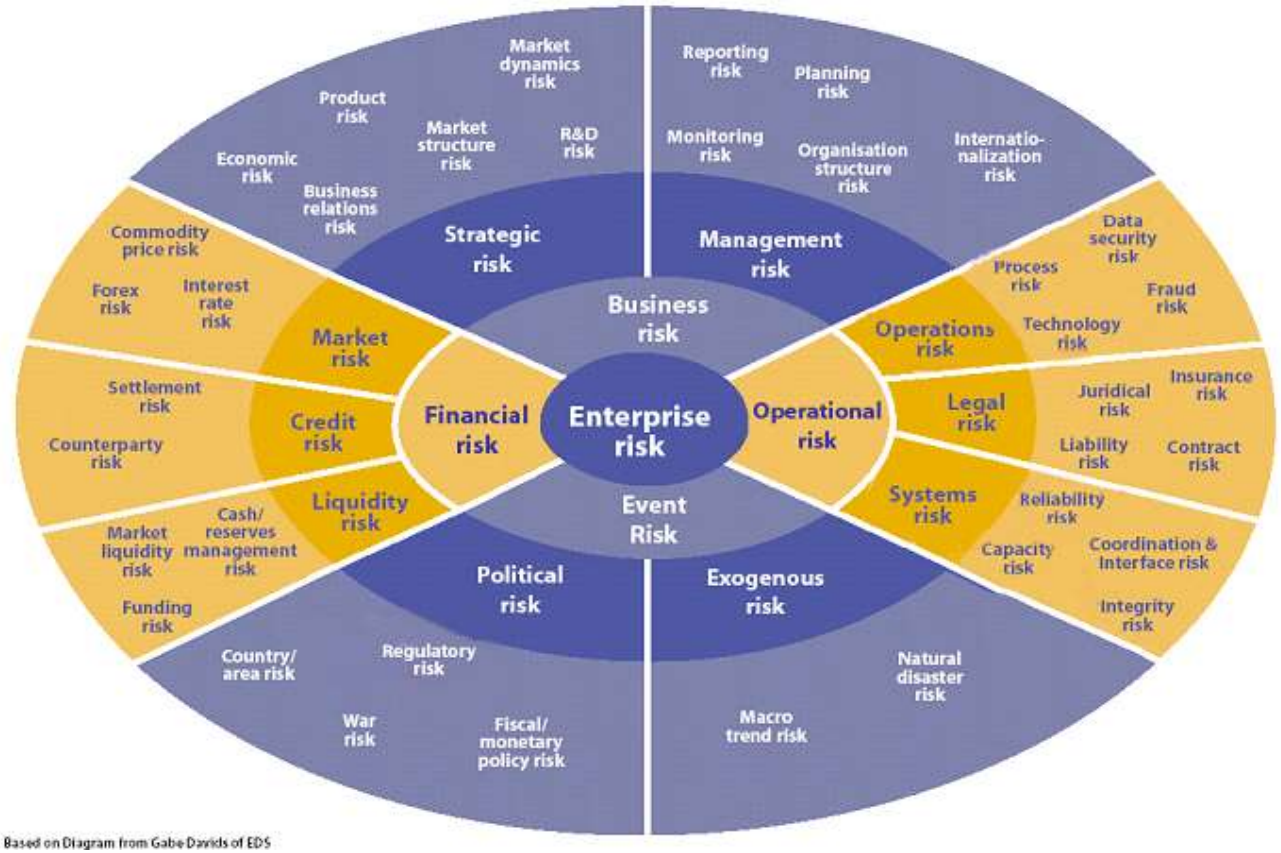
Phishing (using email scams to collect confidential information)

- Key issues: detection, shutting down bogus sites, customer awareness
- Banks are posting warnings on their public sites, and updating security page information with "Q&A" type of information.

Emergent Complexity : Spam Space as Risk



Structuring Risks
An Organizational Risk Categorization Taxonomy

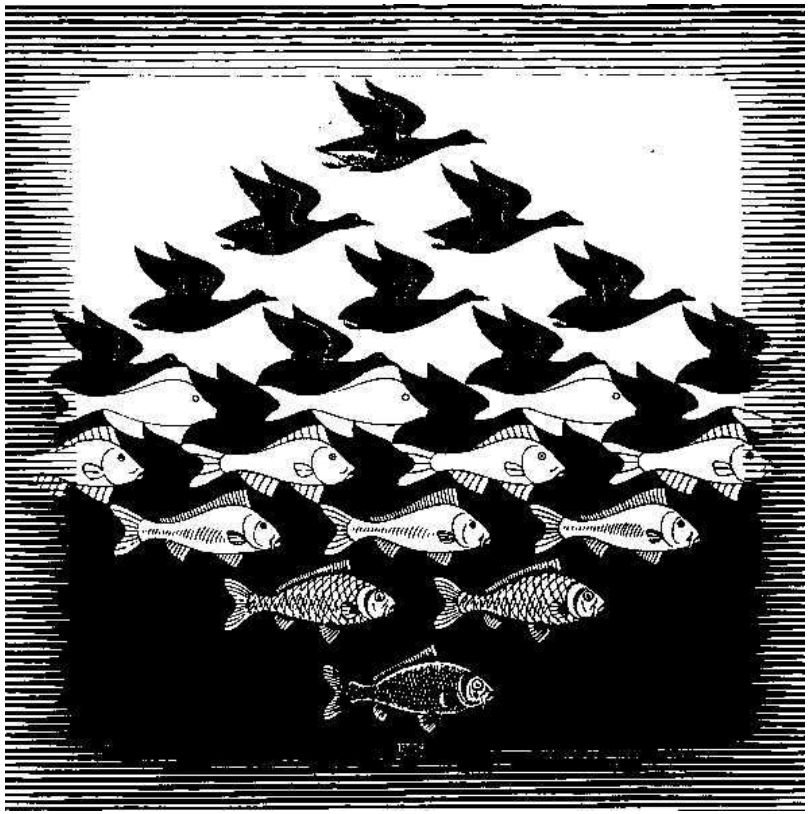


Based on Diagram from Gabe Davids of EDS

Structuring Risks
Regulatory Environment: where are the controls ?

- Personal Information Protection and Electronic Documents Act (PIPEDA) - Canada
- Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) - U.S
- California Law SB1386 - California
- HIPPA (Health)
- Office of the Superintendent of Financial Institutions (OSFI) – Canada - Guideline B10
- The Financial Services Authority (FSA) – England - OS Section 4
- Federal Financial Institutions Examination Council (FFIEC) - U. S.
- Office of the Comptroller of the Currency (OCC) - U.S. OCC 2001 - 47
- The Bank Act - OSFI – Canada – Guidelines B6, B7, B10
- Federal Financial Institutions Examination Council (FFIEC) - U.S. SP-5 Policy
- Sarbanes- Oxley Act (SOX) - U.S.
- Bill 198 - Canada
- SEC Rule 17a-4
- Basel II Accord
- European Union Directives on Information Security
- Canada's National Security Program
- Patriot Act - US

Privacy

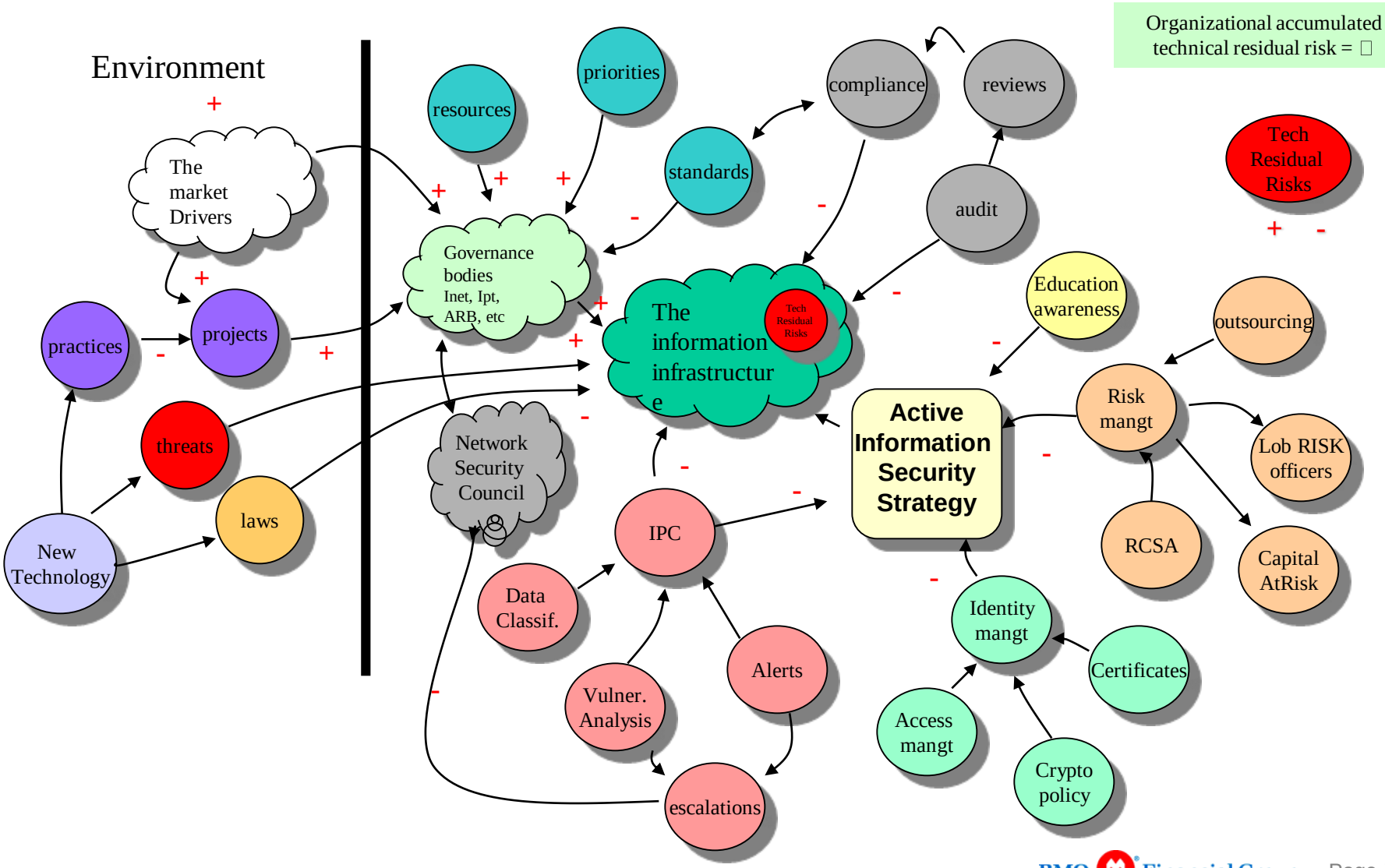


Security

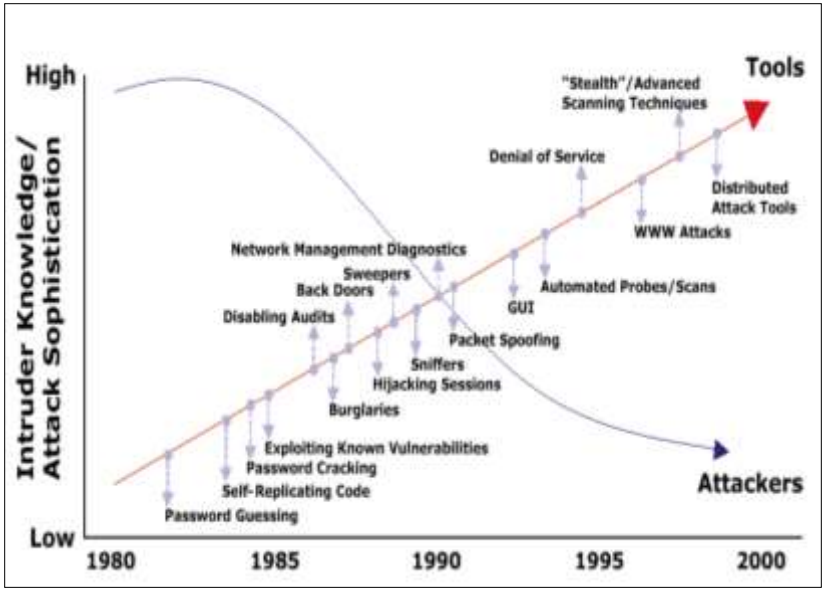
Regulatory Penalties & Fines Grid

Name of Regulatory Mandate	Some Potential Penalties	Potential Fines
SOA	20 years in prison	$15 million
Basel II	Regulatory agency penalties: vary by G-20 country	Regulatory agency fines: vary by G-20 country
HIPAA	10 years in prison	$250,000
GLBA	10 years in prison	$1 million
Patriot Act	20 years in prison	$1 million
Dod 5015.2	Failure to qualify for DoD contract; Contract breach; FAR penalties	Contract penalties
California SB 1386	Unfair trade practice law penalties: vary by state	Private civil and class actions; unfair trade practice law fines: vary by state
SEC Rule 17a-4	Suspension/expulsion	$1 million+

Emergent Behaviors:
An Ecological View of Organizational Risk

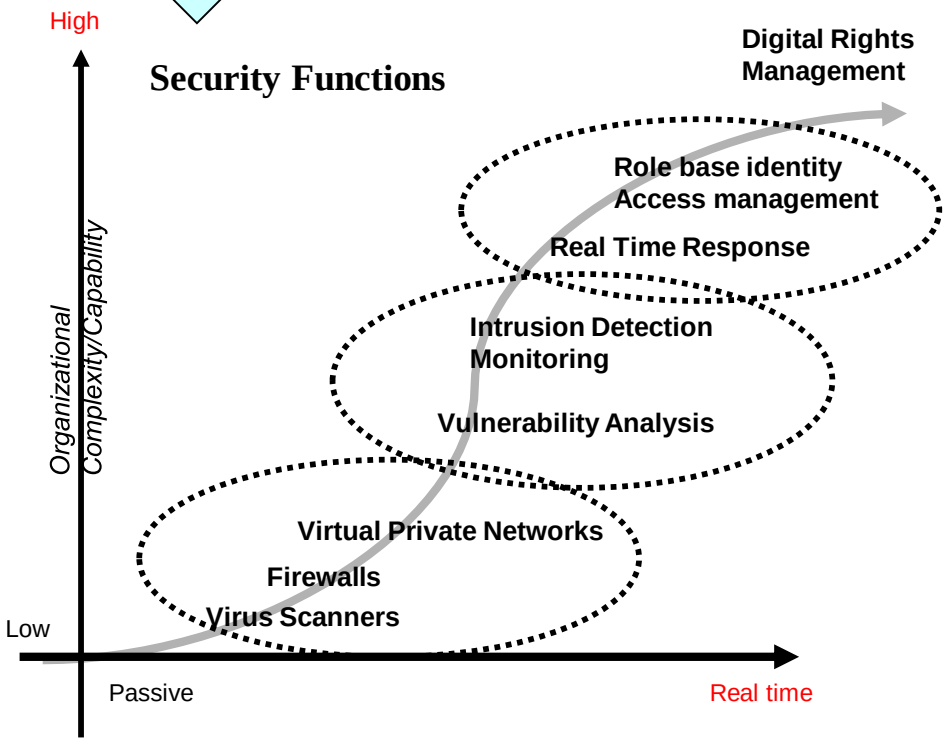


Information Security organization as result of the knowledge transfer process

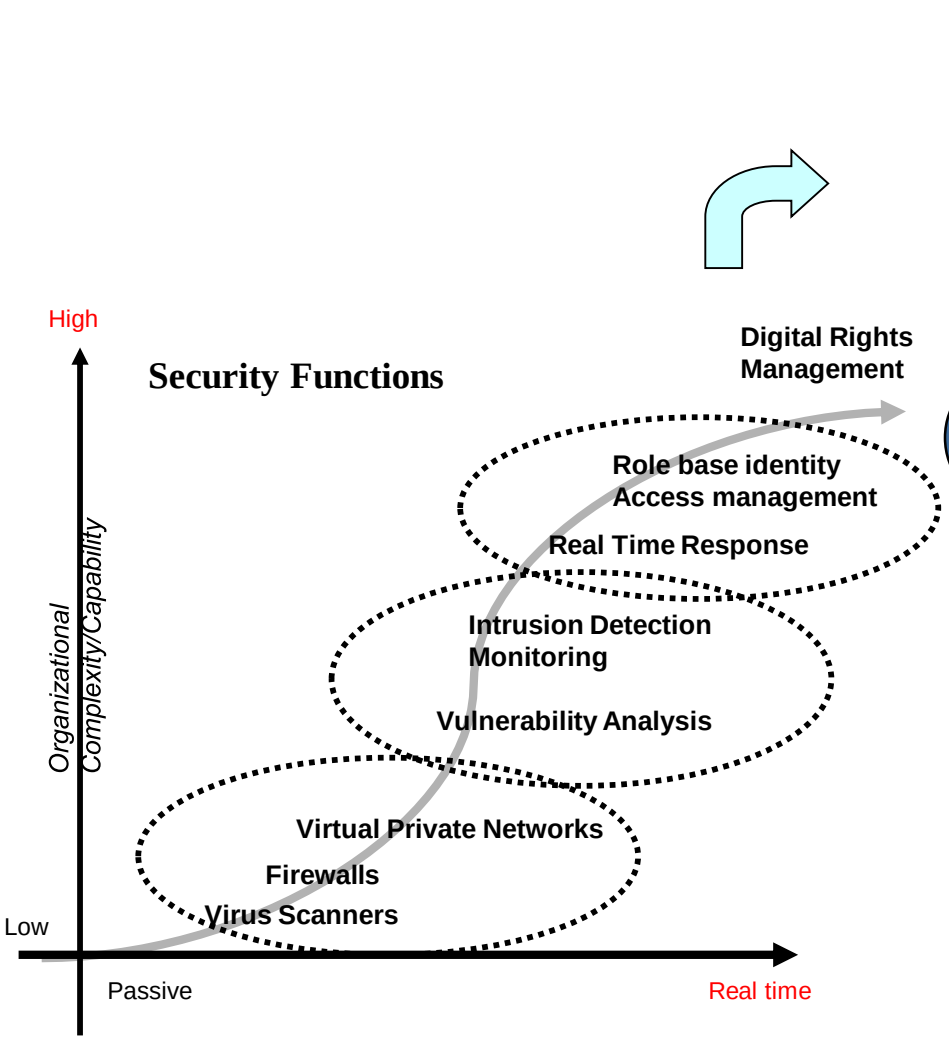


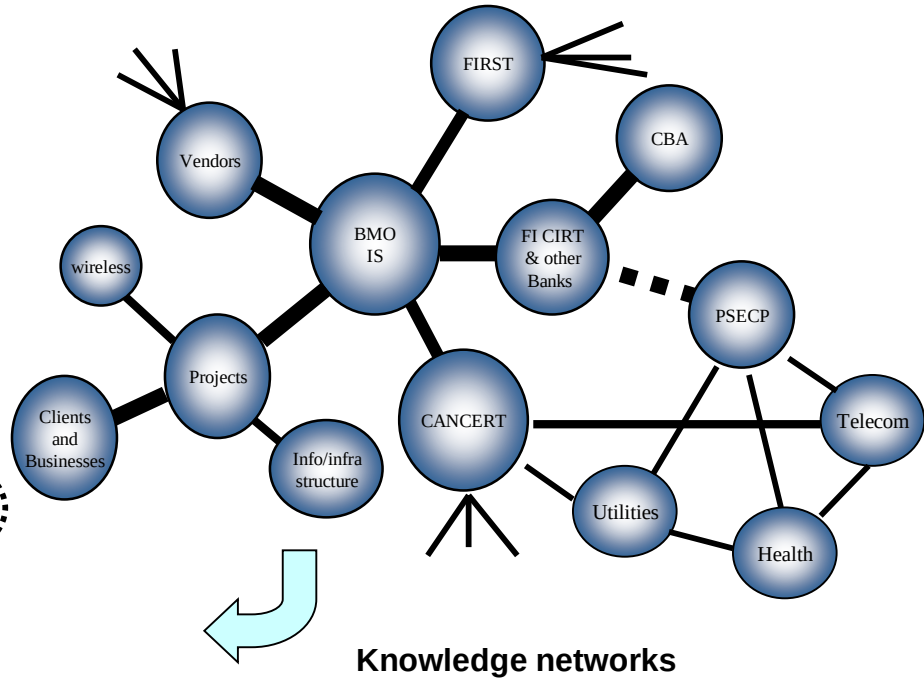
Technical Threats

The Knowledge Transfer Cycle



Knowledge transfer

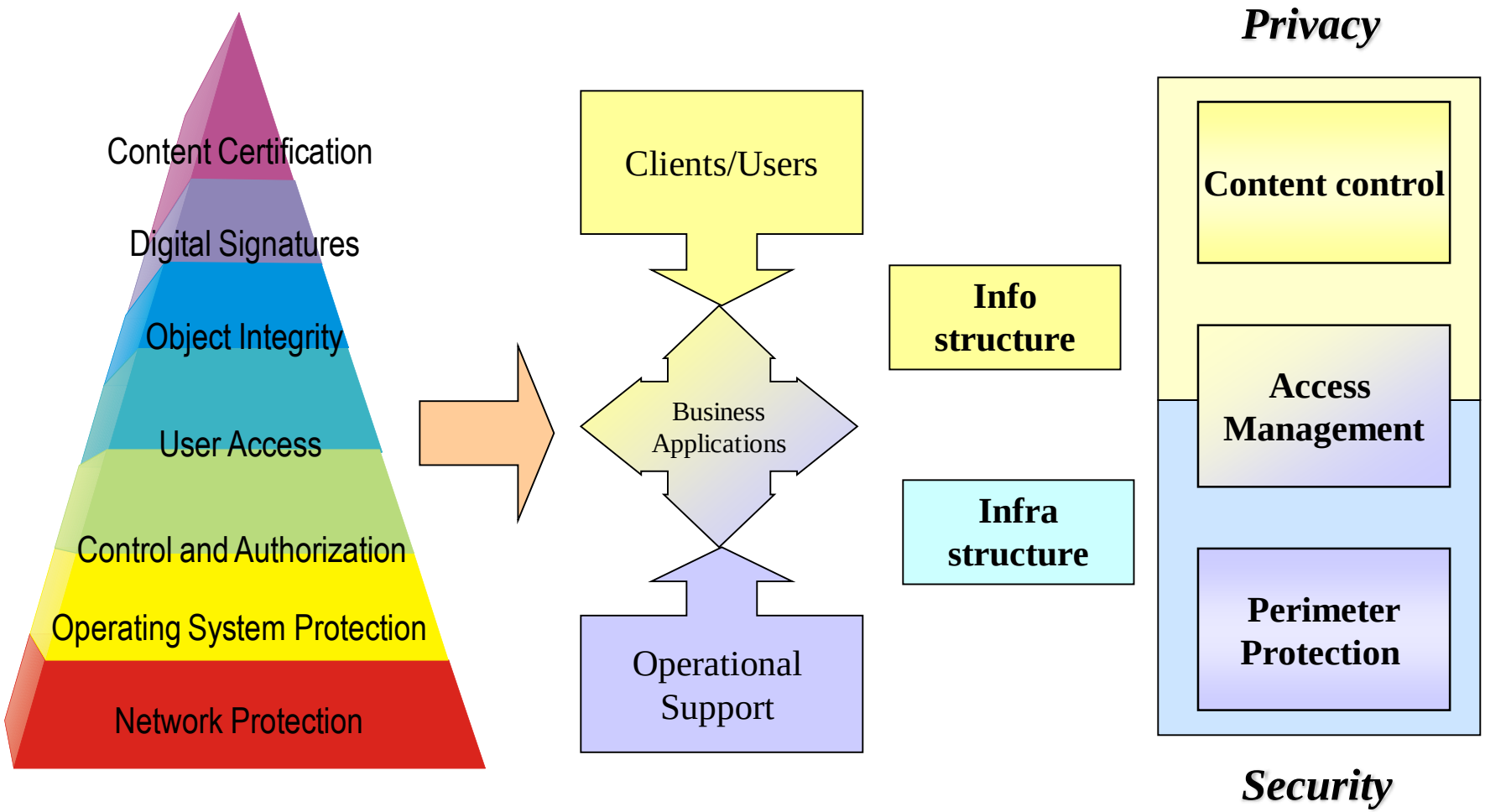




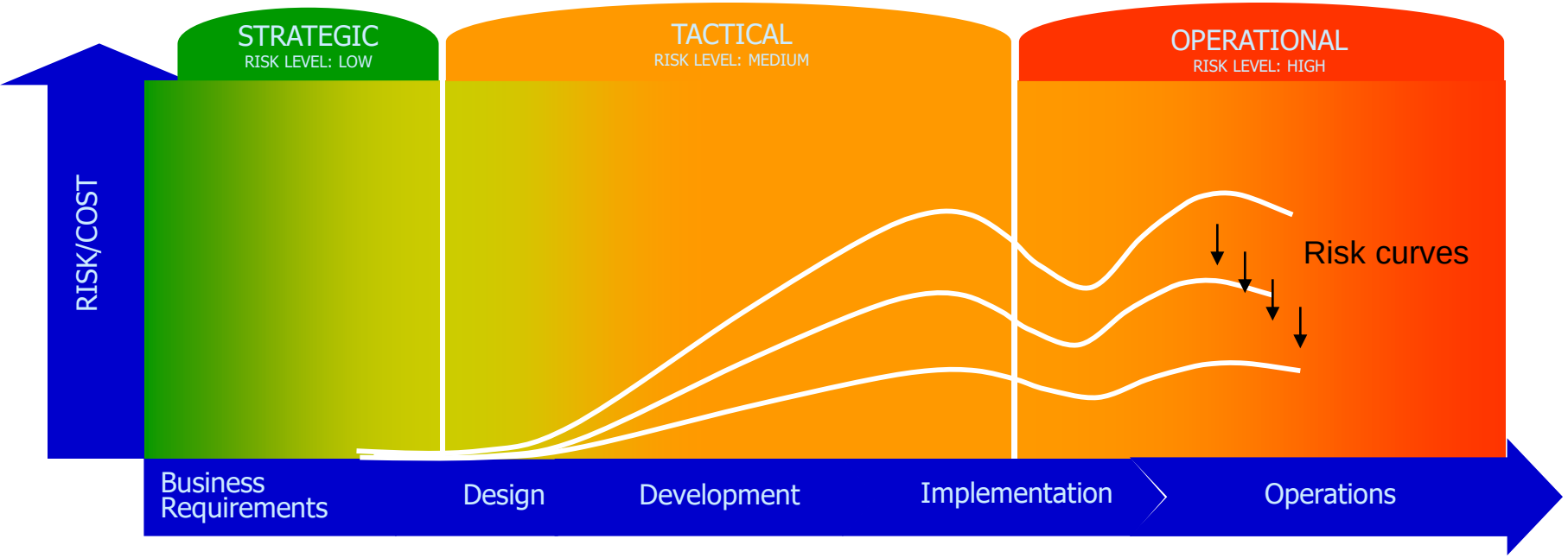
Knowledge networks

The Knowledge Transfer Cycle 2

Control Framework is a hierarchy of accountability structures



Information Security Management Framework



STRATEGIC	TACTICAL	OPERATONAL	OPERATONAL
Governance and policies • Policies • Standards • Procedures • Guidelines • Awareness • Research	Application/system development and deployment • Design reviews • IS solutions • Due care • Risk acceptance • New technology insertion	Active security posture • Antivirus management • Vulnerability assessments • Intrusion detection • Incident response	IS services • Access management • Key management • Security token management • Other operational services

Information Security Key Performance Indicators

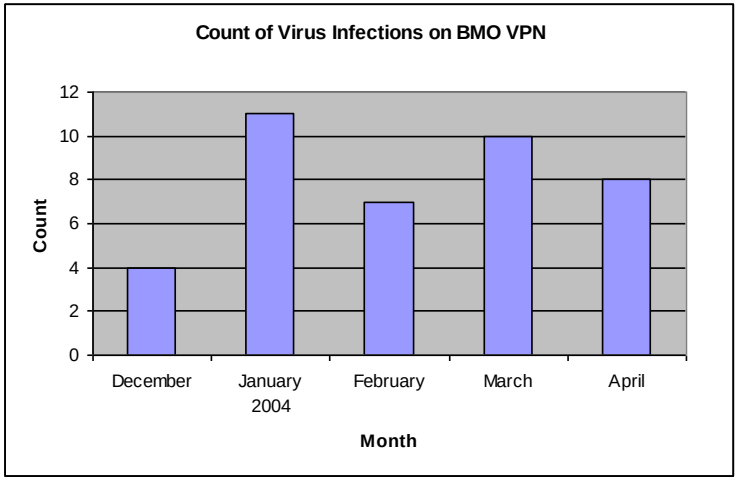
Policy
- Number of Policy Exceptions
- Number of Risk Acceptances
- Value of Residual Risk

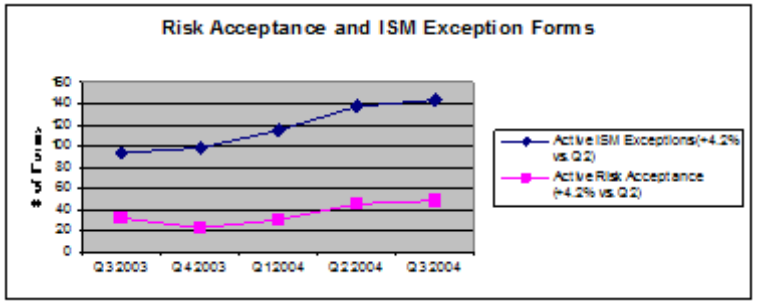
Process
- Number of security issues in new projects
- Number of ID accounts (active/dead)
- Number of keys / digital certificates / tokens
- Time to respond to patches, incidents
- Losses due to security incidents

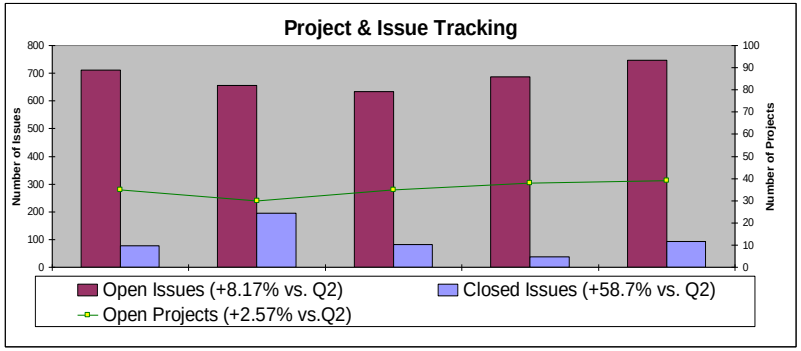
People
- Number of certified personnel
- Overall capital investment ratio security to IT spend
  - per system
  - per person
  - per incident

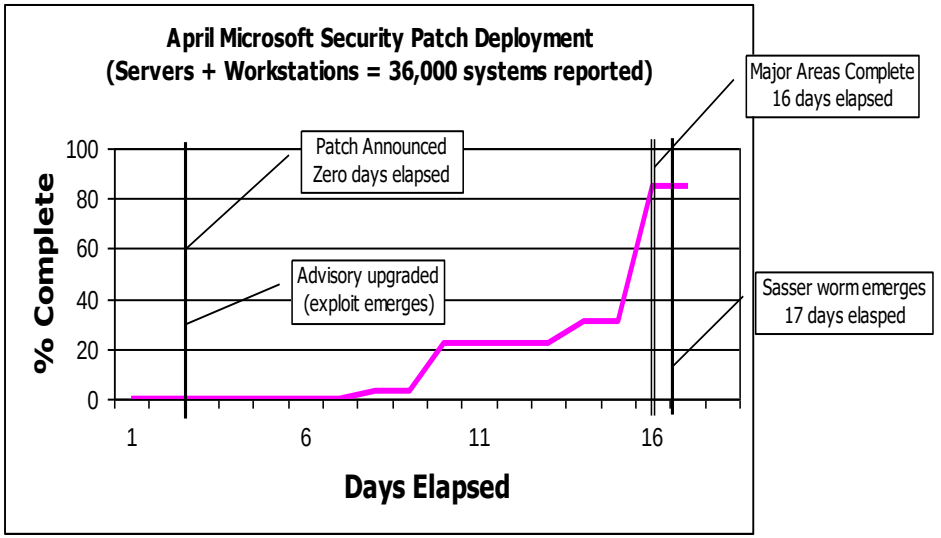
Tycho Brahe (1546-1601)

Information Security Key Performance Metrics

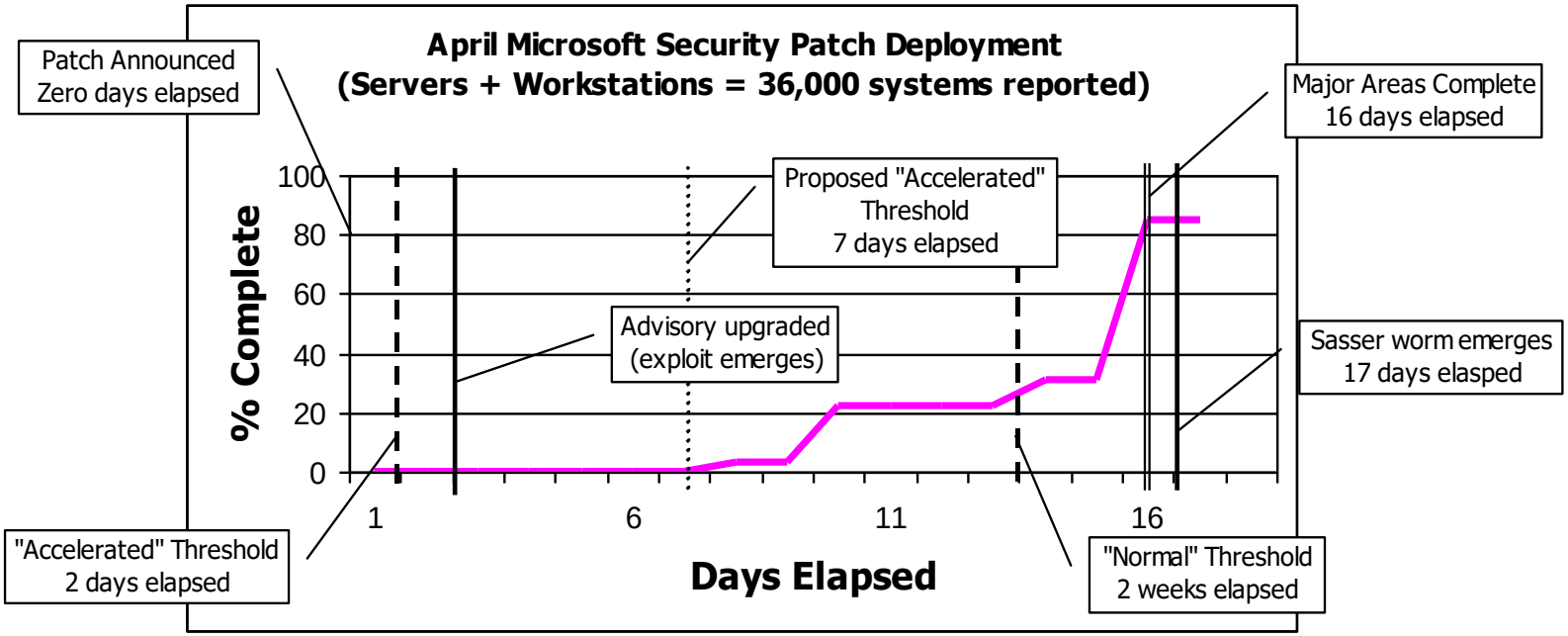





Project & Issue Tracking
Number of Issues
Number of Projects
Open Issues (+8.17% vs. Q2)
Closed Issues (+58.7% vs. Q2)
Open Projects (+2.57% vs.Q2)



Microsoft Patch Deployment



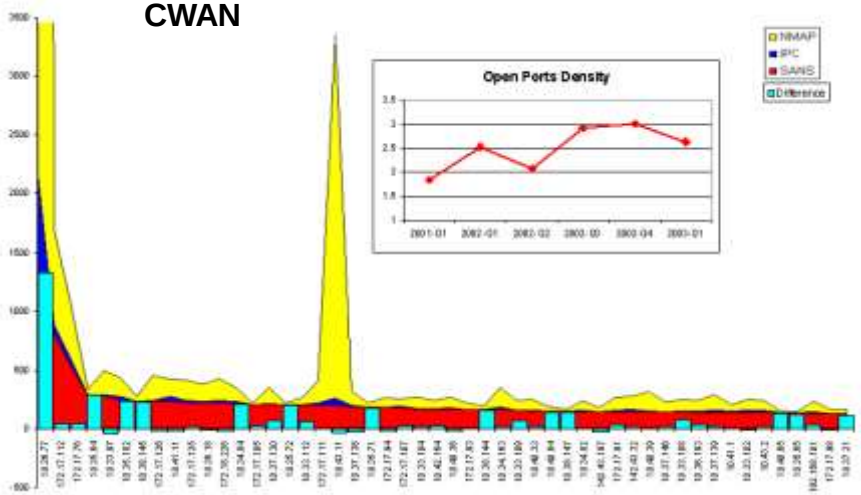
Historical Trend Analysis				
Patch/Incident	**April 2004 Critical (4)**	**February 2004 Critical**	**Nachi/Blaster (August 2003)**	**SQL Slammer (January 2003)**
Days to Patch (90% Complete)	**16**	**9**	**34**	**209**

Note:
April 2004 release required 4 separate patches

	H	M	L
H	Emergency	Accelerated	Accelerated
M	Accelerated	Accelerated	Normal
L	Accelerated	Normal	Normal

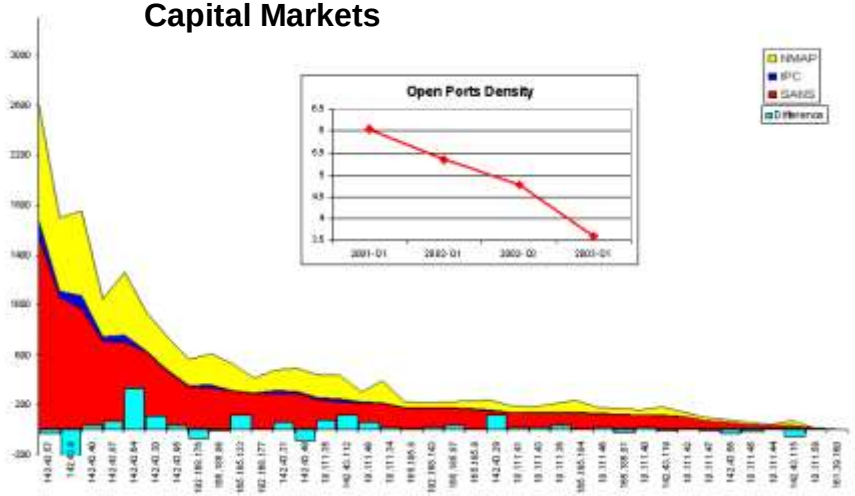
Active security posture – Vulnerability Analysis results

CWAN

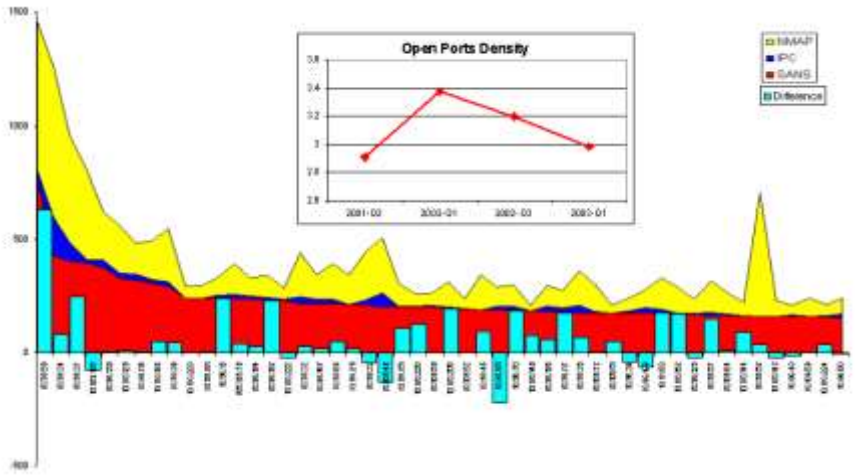


	Major Networks				
Year/Quarter	CWAN	BWAN	Nesbitt Burns	Capital Markets	Harris
2001	1.84		2.91	6.04	3.35
2002 – Q1	2.53		3.38	5.34	2.04
2002 – Q2	2.08				1.84
2002 – Q3	2.93		3.19	4.77	
2002 – Q4	3.01	2.41			2.35
2003 – Q1	2.63		2.98	3.59	

Capital Markets



Nesbitt Burns



Quarterly Information Security Dashboard

Information Security Group	Information Security Service	Details on Page	Enterprise		
			Posture	Forecast	Last Q
Security Practices & Technology	IS Policy & Strategy	6			
	Standards & Architecture	7			
	Project Assessments	8			
	Training	9			
Information Protection Centre	Anti Virus	11			
	Vulnerability Assessment	12			
	Intrusion Detection	13			
	Response/Management	14			
Information Security Operations	Key Management	15			
	Encryption (PKI)	16			
	Access Management	17			
	CSPIN (devices)	18			
	Remote Access	19			
Business Analytics	Analytics/ reporting	20			
	Education & Awareness	21			

Legend

=Key Issues

=positive trend

=negative trend

=stable

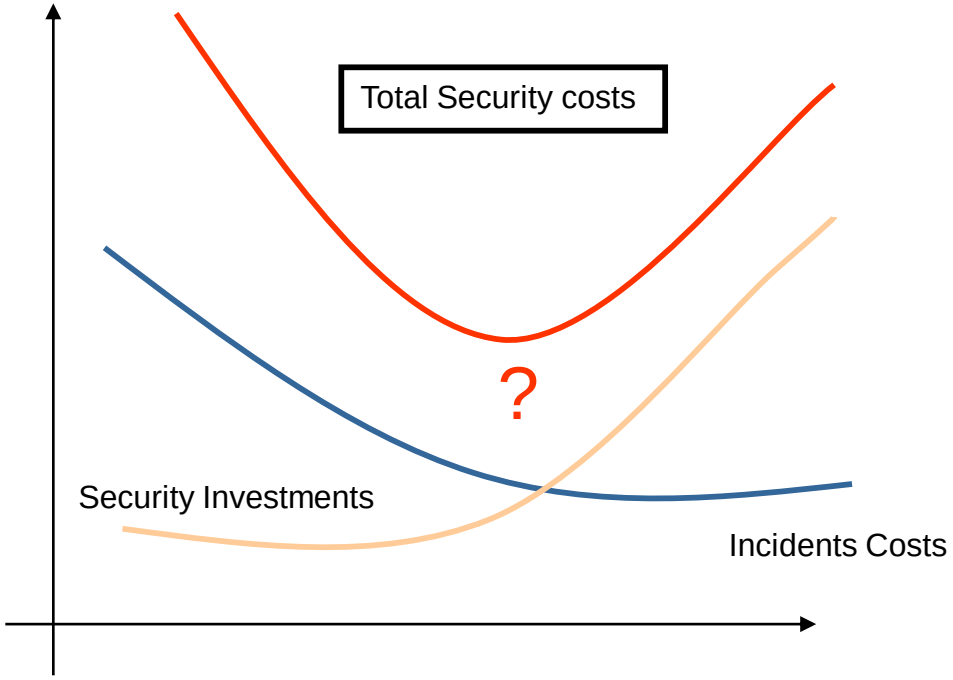
= unsatisfactory

= fully satisfactory

Making The Case for Security Investments

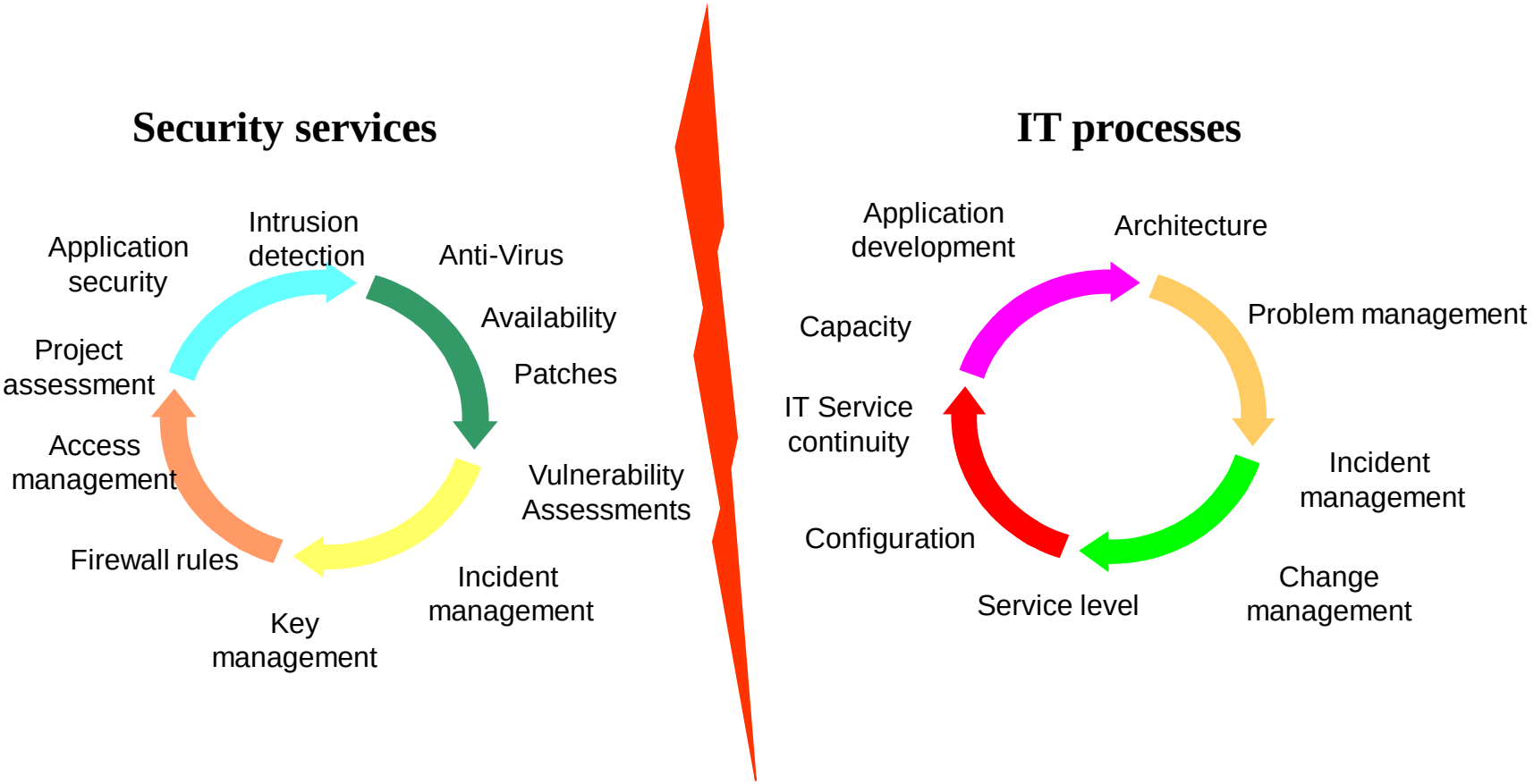
Return on Investment (ROI) has failed to demonstrate it economically because there are too many variables

- Benefits hard to quantify: what's the value of good health?
- Statistical data unreliable and changing fast
- Cost avoidance not the same as cost savings
- The "language divide": accounting vs. security
- Loss of credibility more costly than loss of physical assets
- Technology substitution is not a guaranty of more capability



The Security Challenge: Alignment

The Digital Divide
Two solitudes, in virtual isolation



Maturity Framework Levels: Stages of Evolution of a system

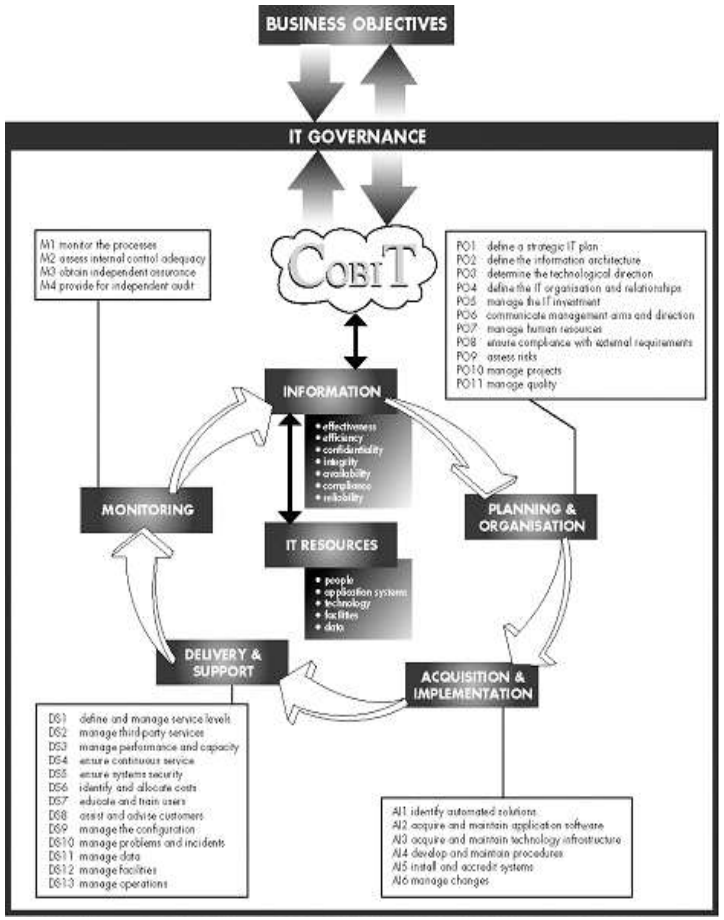
Phase	*Description*
0. Absence	Nothing present
1. Initiation	Concrete evidence of development
2. Awareness	Resources allocated
3. Control	**Formalized**
4. Integration	Synergy between processes
5. Optimization	Continuous self improvement & optimization

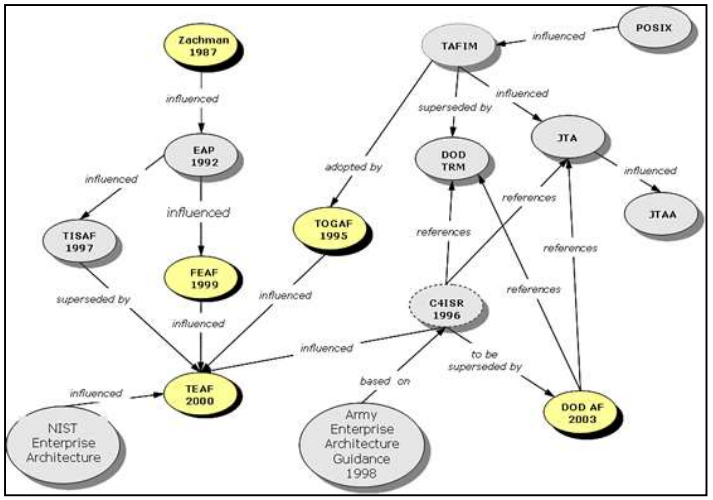
Characteristics:

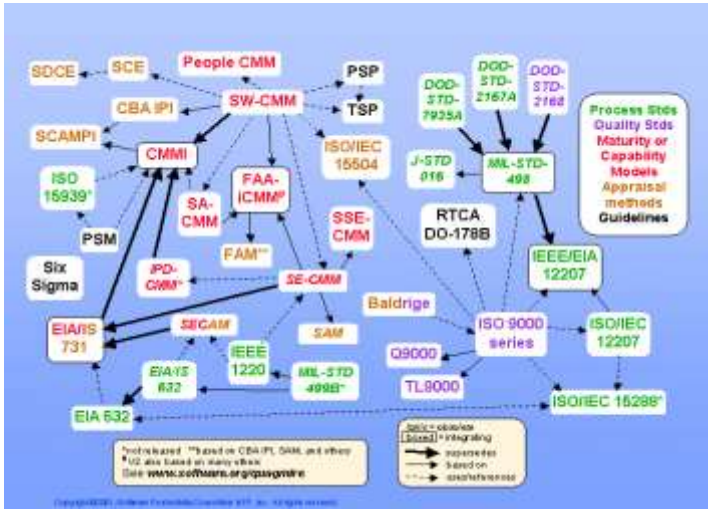
visible results

management reports
task/authorities defined
active rather than reactive
documentation
formal planning

Maturity Frameworks pedigree : The reference framework







It is better not to proceed at all than to proceed without method

Descartes

Information Security Maturity model - ISO 17799
Information Technology Infrastructure Library (ITIL)
SEI – CMM (Capability Maturity Model)

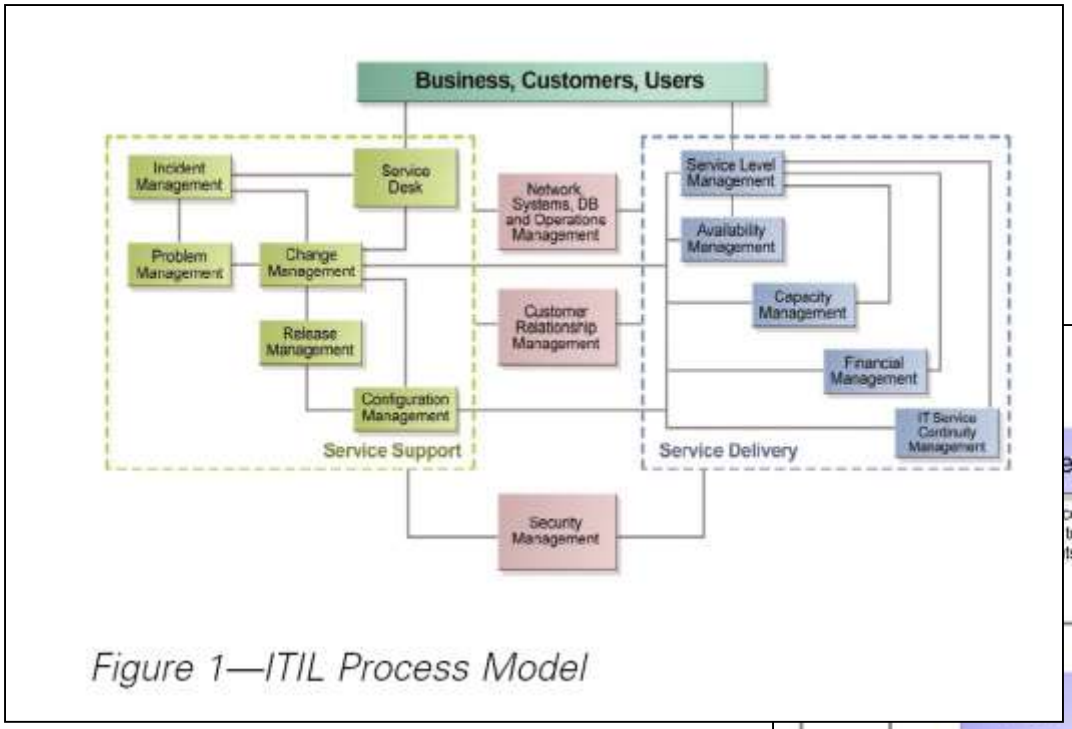
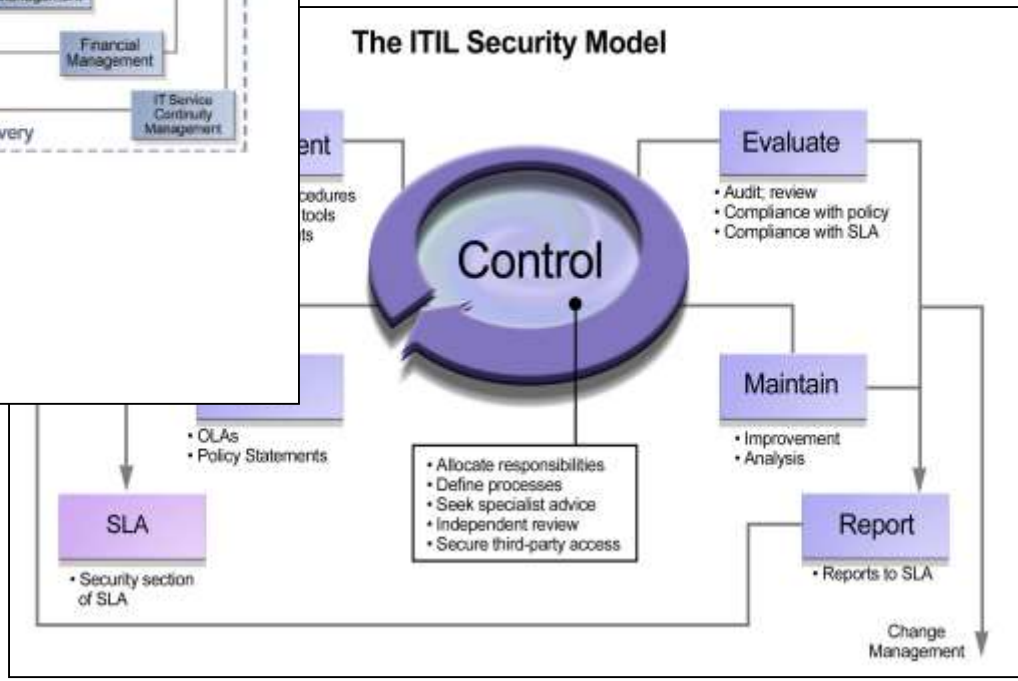
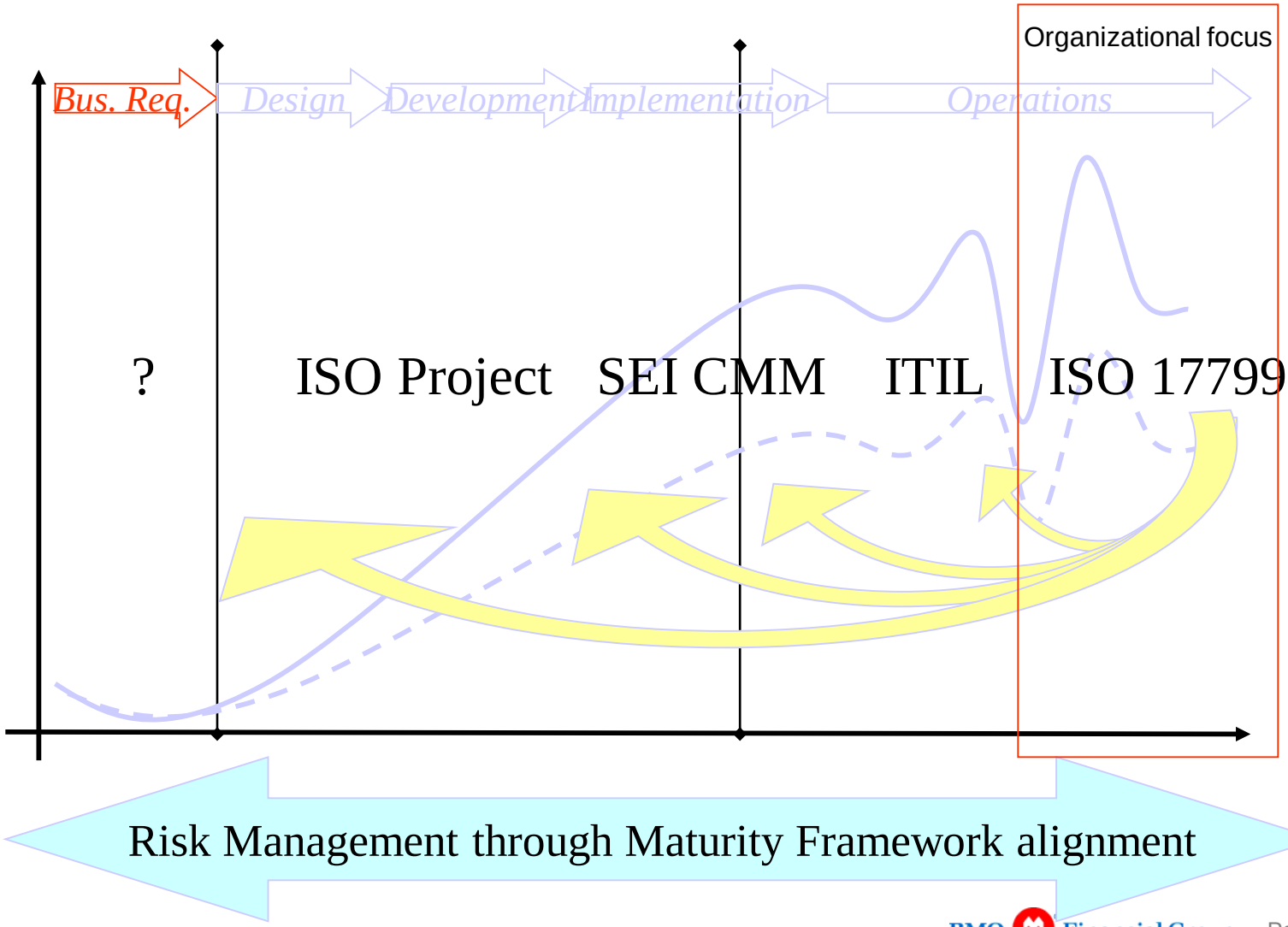


Figure 1—ITIL Process Model

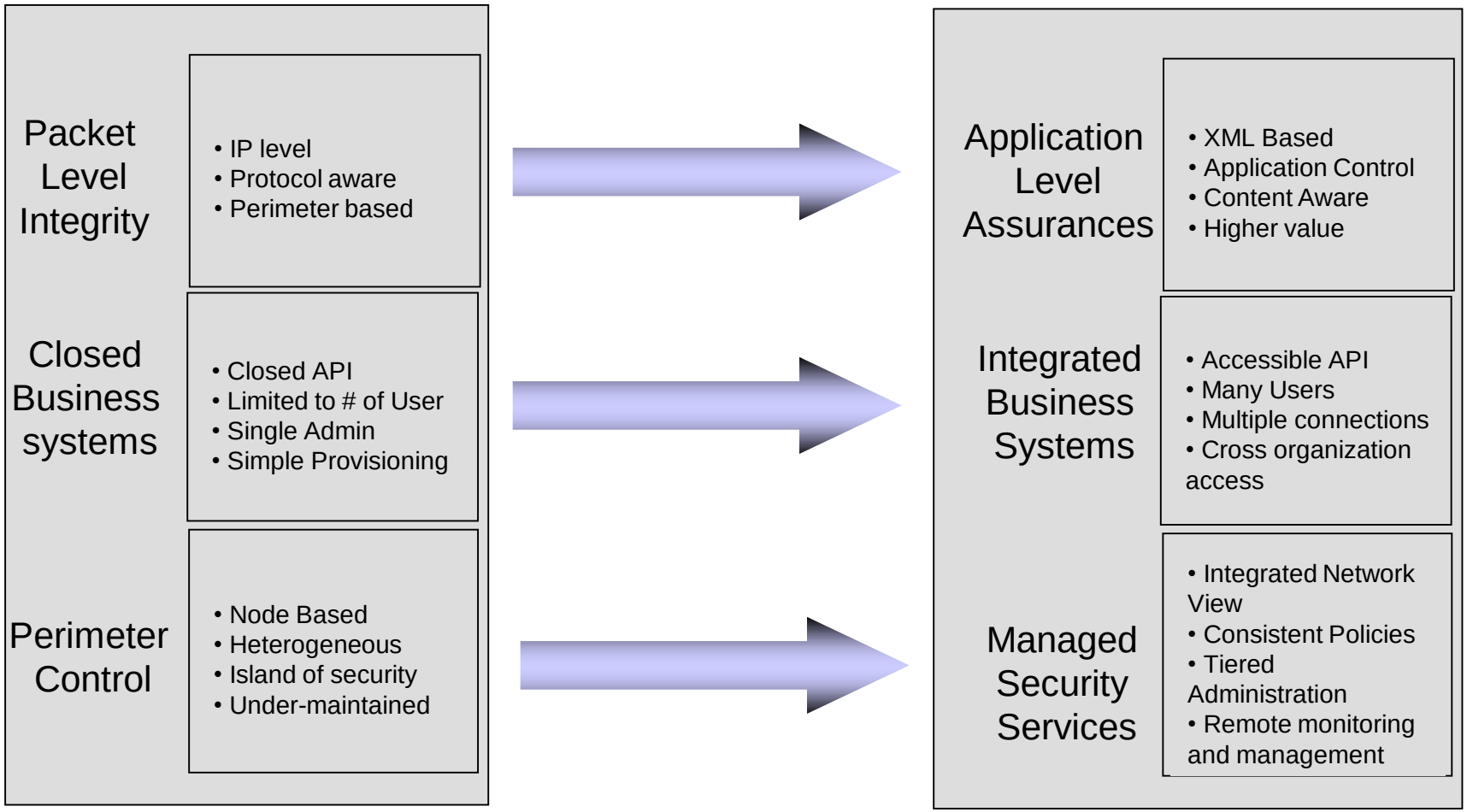


A proposal for a new integrated risk framework

The objective is to lower the overall risk through capability maturity framework integration



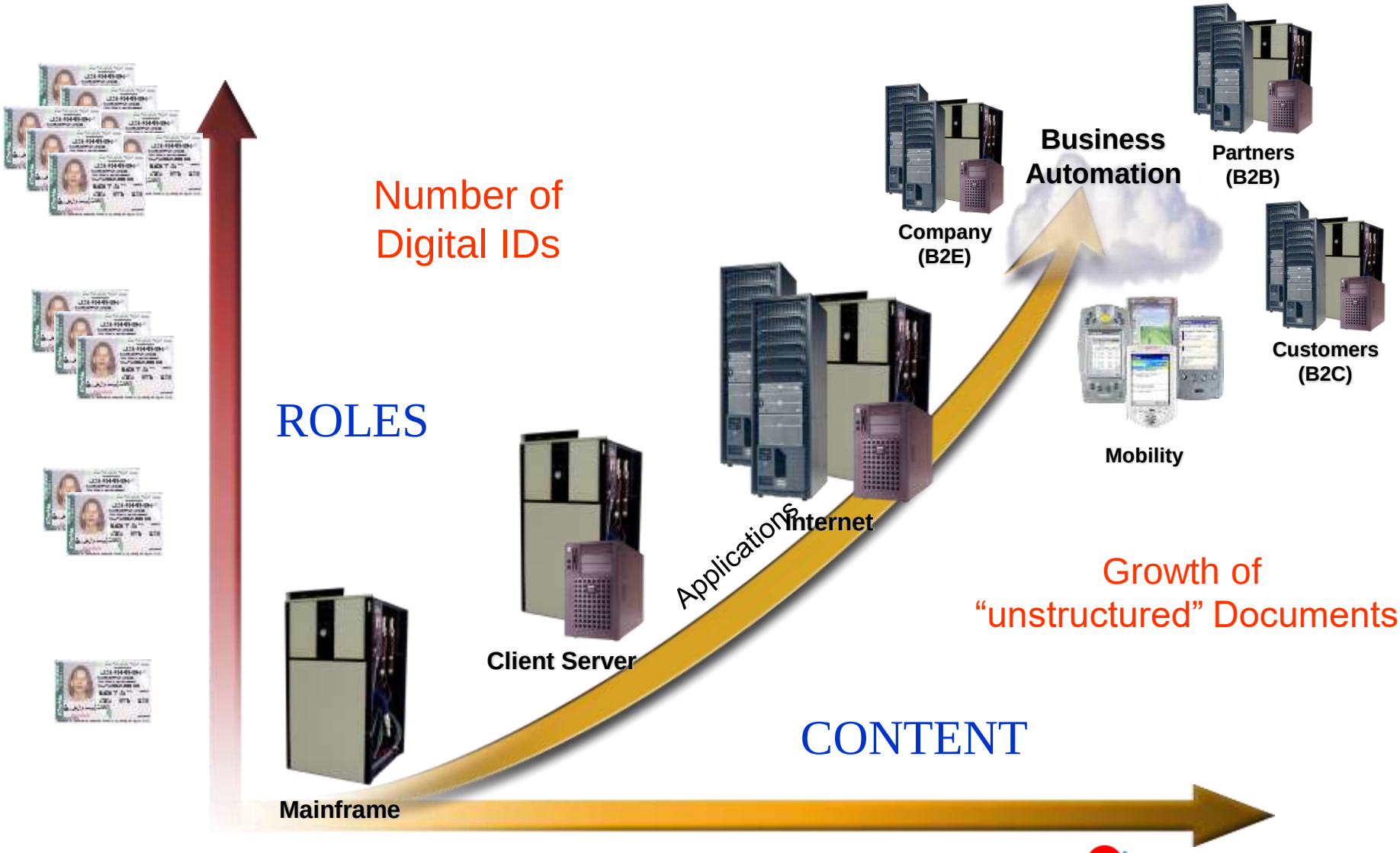
Strategic Evolution of Information Security



Present Security Model

Target Security Model

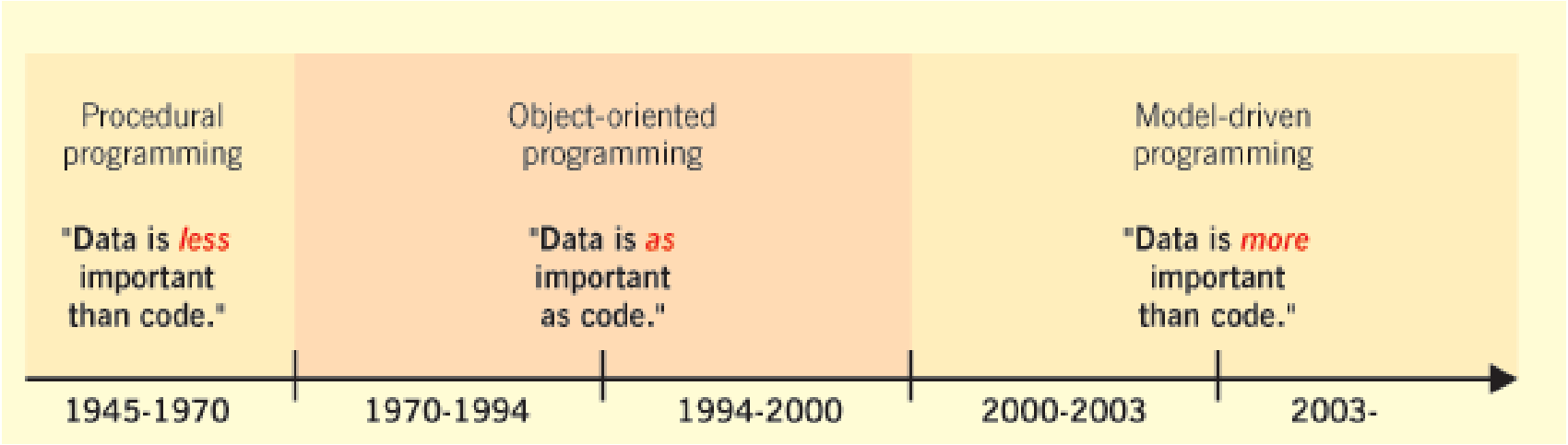
The new Information Security challenge: Managing the "Roles and Content" via "Rights and Privileges"



Information centric organization

- Content increasingly easy to collect and digitize
- Has increasing importance in products and services
- Is very hard to value or price
- Has a decreasing half life
- Has increasing risk exposure
  - –integrity-quality
  - –regulation privacy/SOX
- Is a significant expense in all enterprises

(IT Governance – Weill and Ross)

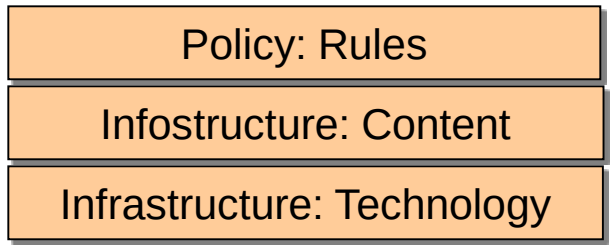


Michael C. Daconta

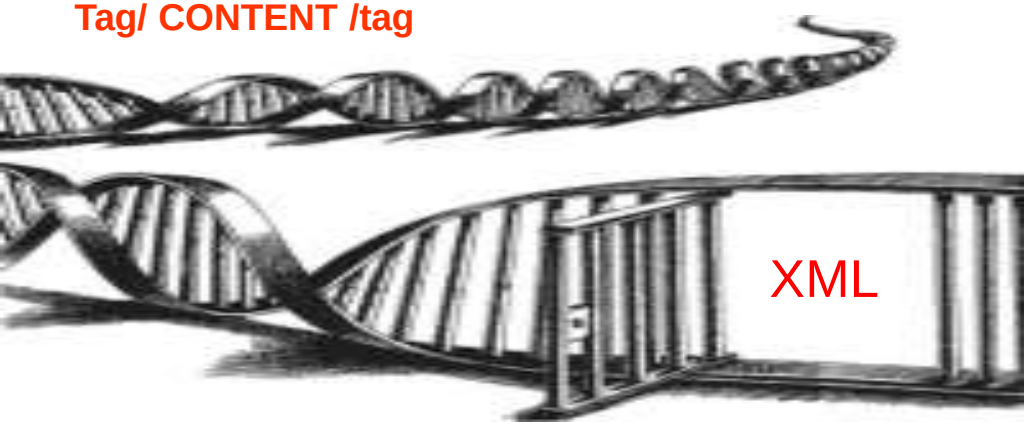
Where are the risk coming from the rise of the info-structure

Where is the locus of control outside the boundaries of the organization ?

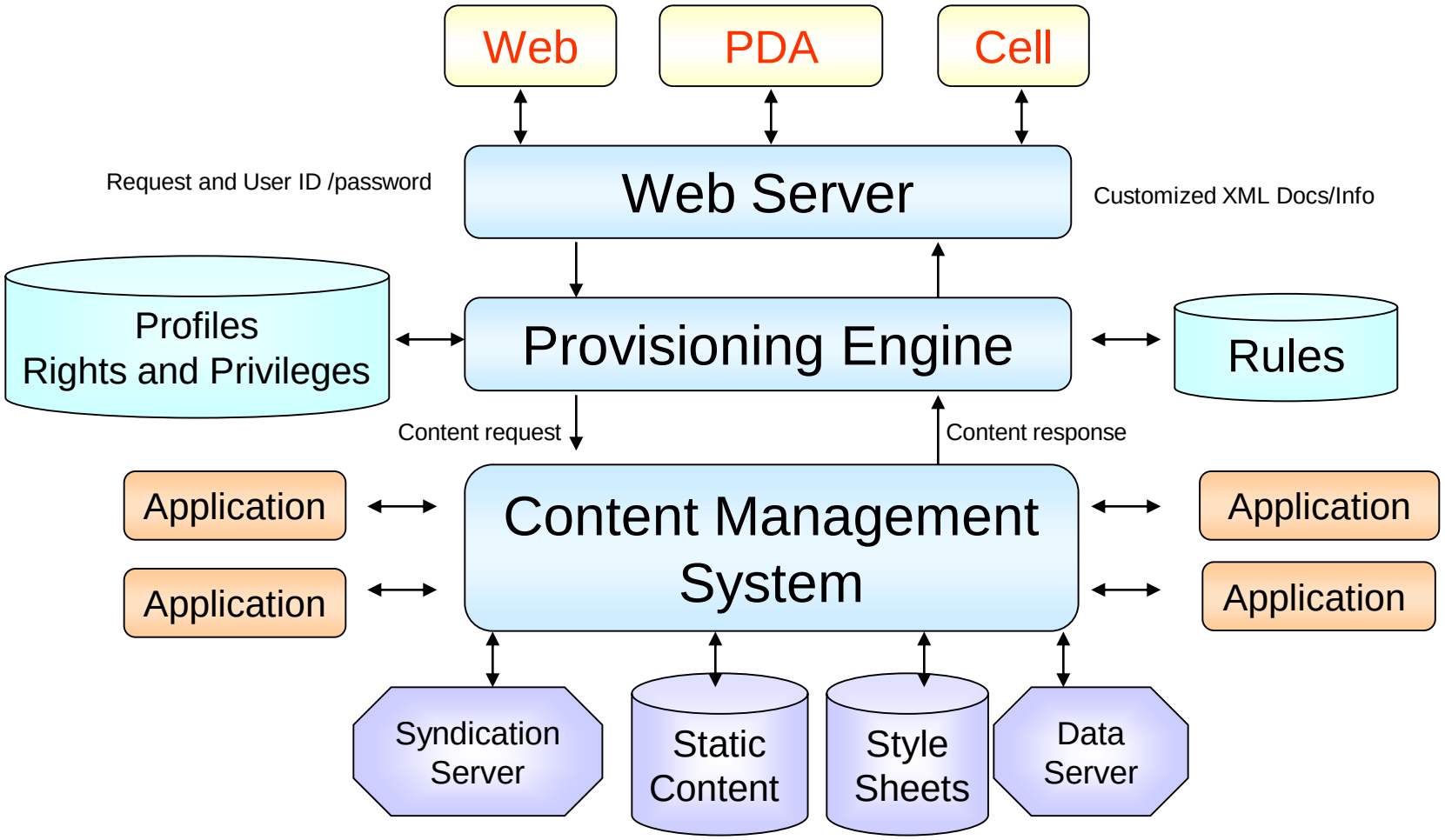
Information Security Management has to recognize a requirement for a content control model that is independent from a specific technical solution.



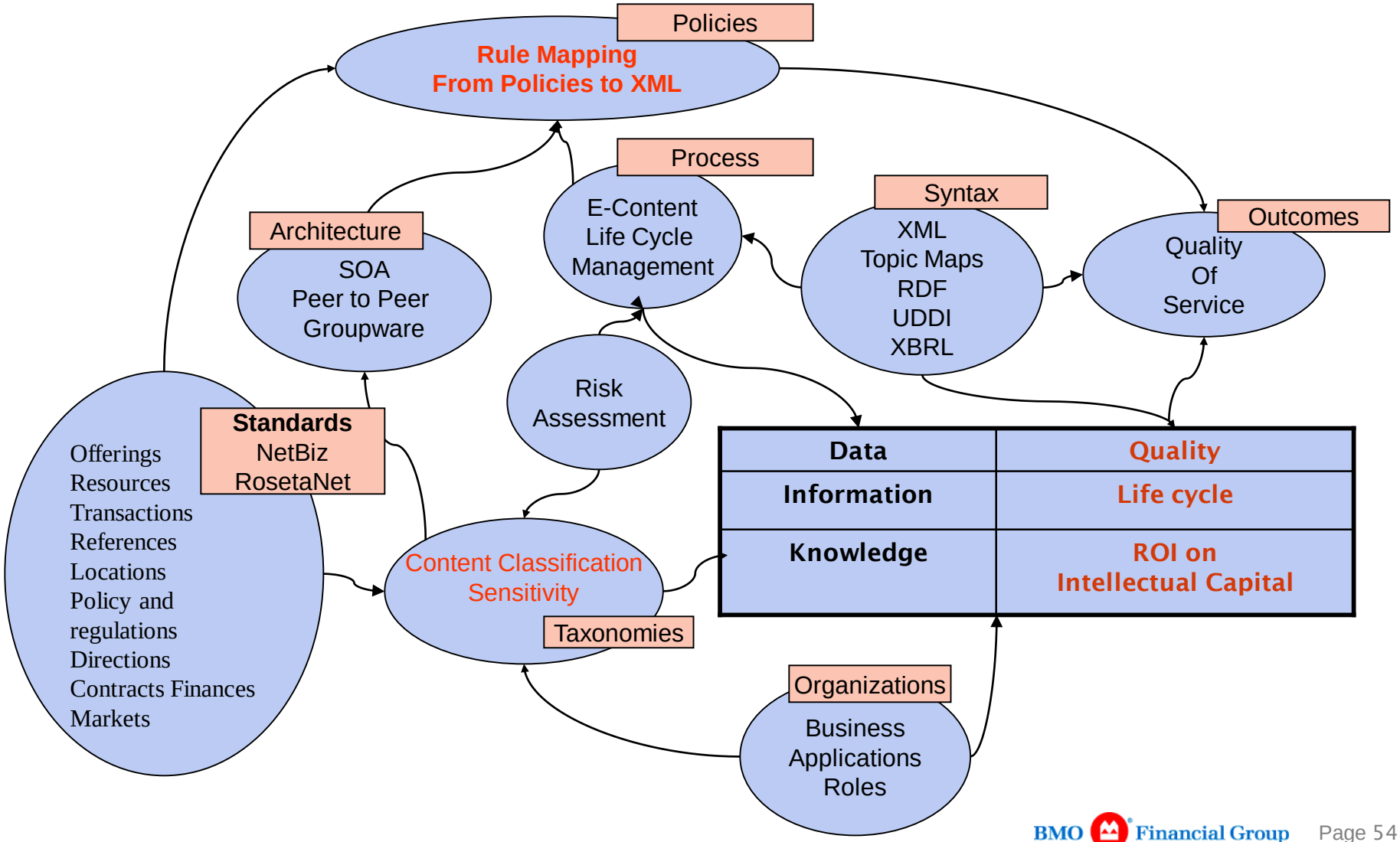
To deal with the new information security risks in "semantics management" Then the focus to content management and issues: Topic Maps, XML, RDF, UDDI, XBRL, SAML, Ontologies, And more and more



The Integrated Architecture : Content and Technology



The Architecture of the Infostructure
The Ontology of Information Management



Information Management as Information Security

NEW IMPERATIVES

Data Classification

Information stewards

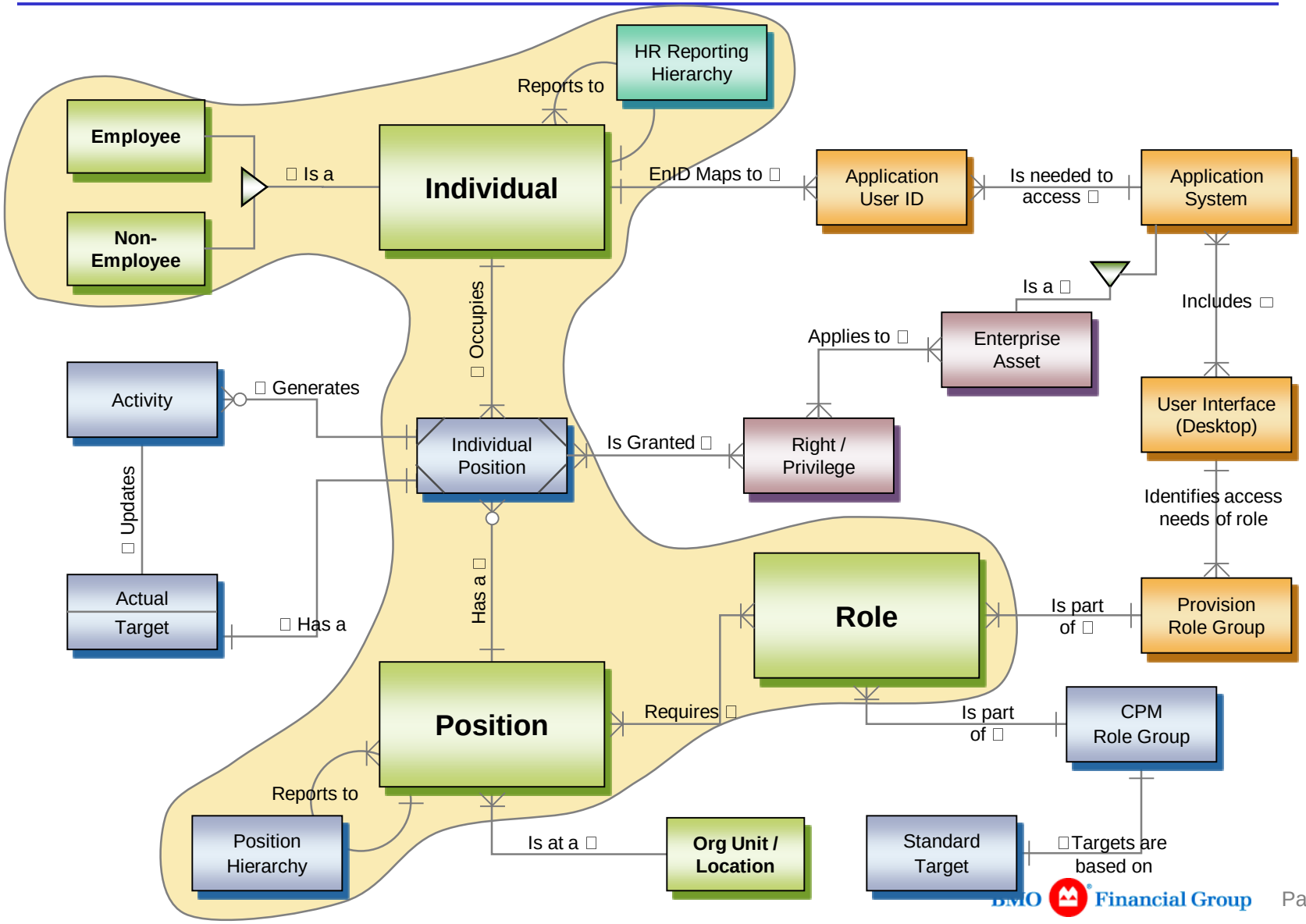
Content lifecycle management

Identity Management

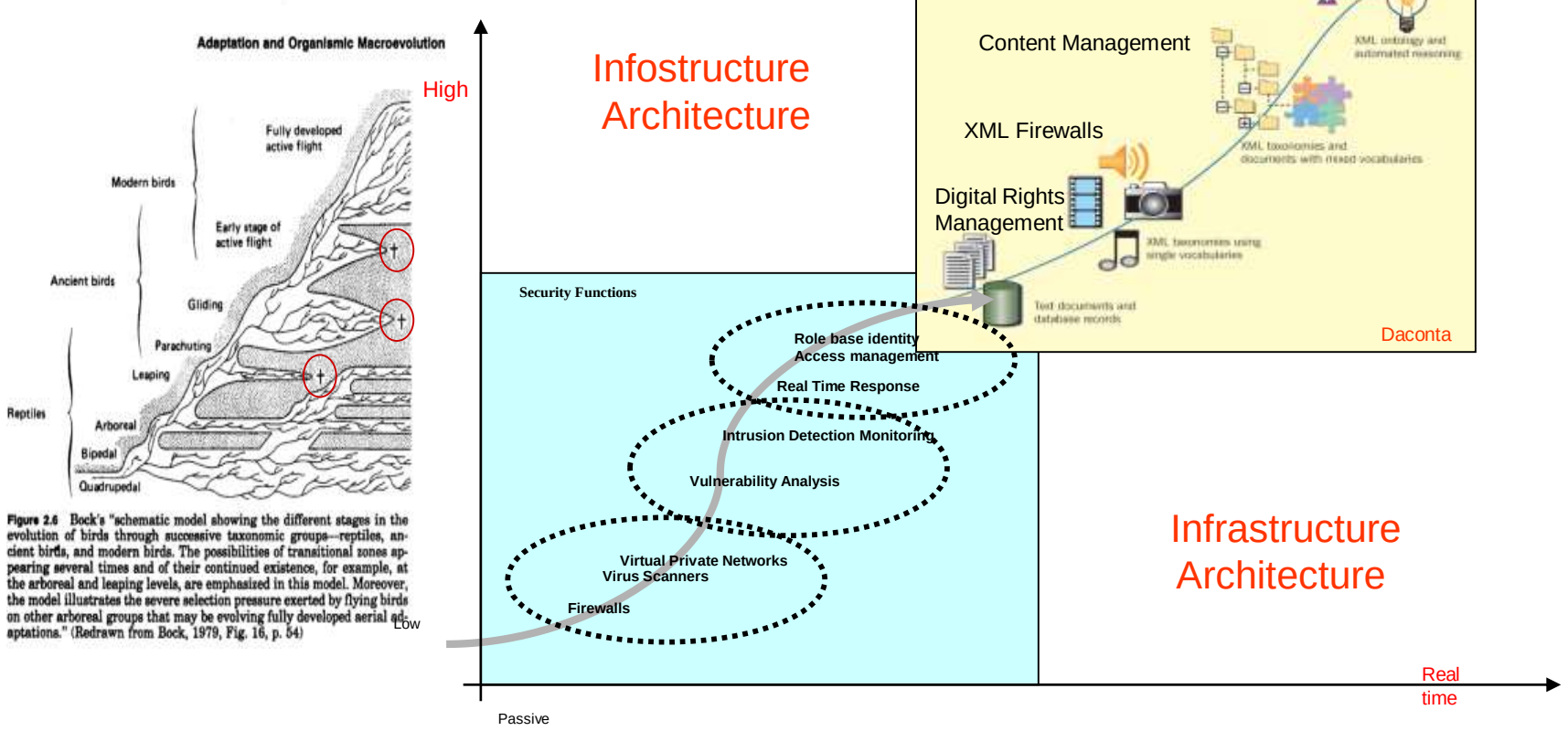
Digital Rights Management Services

	Examples of content	Recommended Controls (accumulates as you go down)
Public	News clippings Market Data	Contracts, Licensing, usage and log files for activity purpose
Internal	Policy documents Routine Procedures	Assets should be labeled with Classification Log files Broad Access Control
Confidential	Passwords lists Customer Names Project documentation Customer Snapshots Credit Card Numbers Account Numbers	Encryption – anonymizing - pseudomizing Separation of Duties Secured log files and Access Control Review of Sample Logs Systems involved are assessed periodically and around significant changes Trained and certified people involved in design and operation
Highly Sensitive	Customer public identification associated with account information Customer Data with SIN Strategic Plans	Review and sign off of Logs by stewards and custodians Systems involved are assessed periodically and around significant changes Host/device monitoring for intrusion Trained and certified information security people involved in the review of operations

The New Audit Space
Control of Content : Digital Rights Management



The next level of challenge
Aligning the Infostructure with the Infrastructure


Organizational Complexity/Capability
Adaptation and Organismic Macroevolution
Fully developed active flight
Modern birds
Early stage of active flight
Ancient birds
Gliding
Parachuting
Leaping
Reptiles
Arboreal
Bipedal
Quadrupedal
Figure 2.6 Bock's "schematic model showing the different stages in the evolution of birds through successive taxonomic groups—reptiles, ancient birds, and modern birds. The possibilities of transitional zones appearing several times and of their continued existence, for example, at the arboreal and leaping levels, are emphasized in this model. Moreover, the model illustrates the severe selection pressure exerted by flying birds on other arboreal groups that may be evolving fully developed aerial adaptations." (Redrawn from Bock, 1979, Fig. 16, p. 54)
High
Low
Infostructure Architecture
Semantic Management
Content Management
XML Firewalls
Digital Rights Management
Daconta
Security Functions
Role base identity Access management
Real Time Response
Intrusion Detection Monitoring
Vulnerability Analysis
Virtual Private Networks
Virus Scanners
Firewalls
Infrastructure Architecture
Passive
Real time

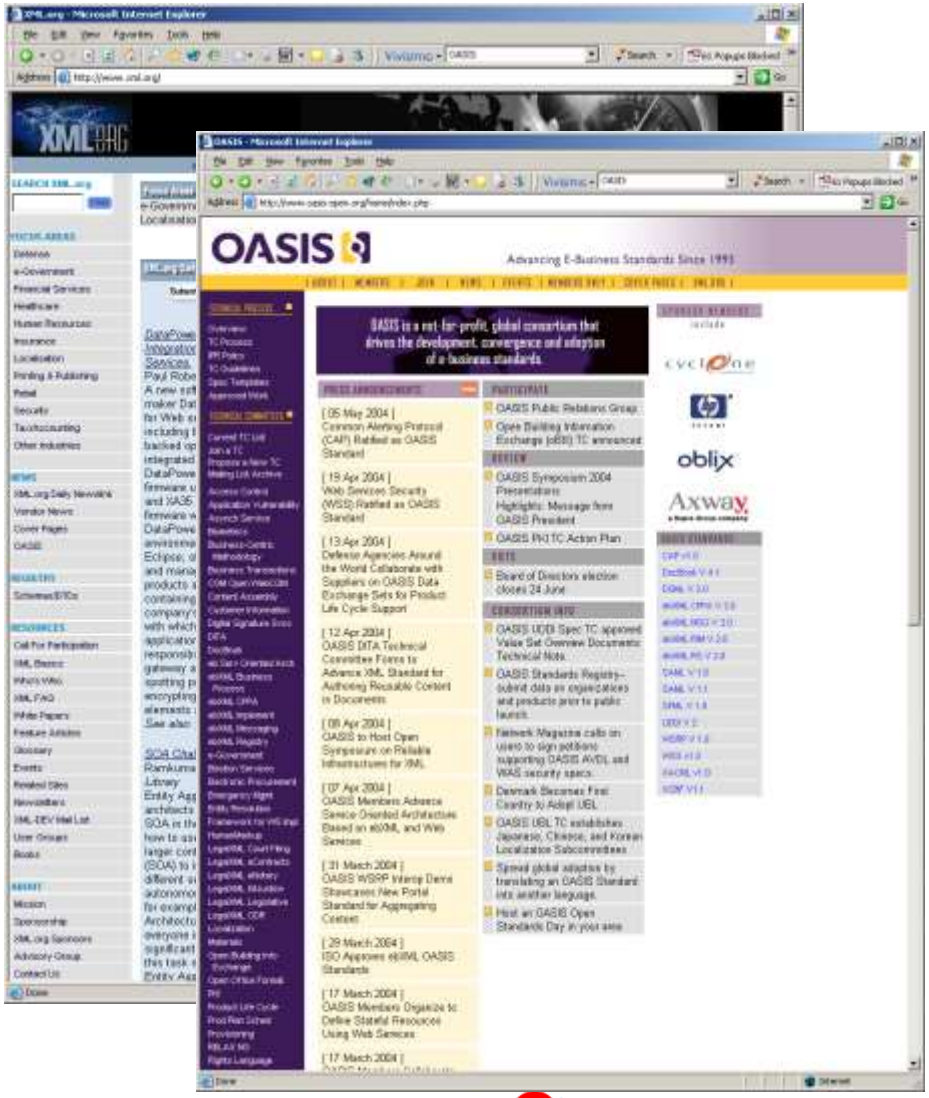
The New Security Debate Space

The B2B market forces are enabling standards.

- B2B models
- Taxonomies and ontologies
- XML Protocols
- WS-Security standards

What protocol and standards drive your business ?

Do you have an Information Security Officer debating these issues ?


XML.org
OASIS
Advancing E-Business Standards Since 1993
OASIS is a not-for-profit, global consortium that drives the development, convergence and adoption of e-business standards.
oblix
Axway

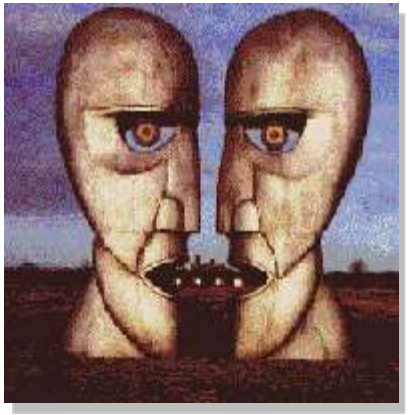
The Role of the Chief Information Security Officer

1. Information Risk identification
2. Information Risk formalization
3. Development of practices and tools
4. Integrate “root cause” analysis into governance framework
5. Devolve processes from exception management into operations
6. Improve Information asset identification and management accountability

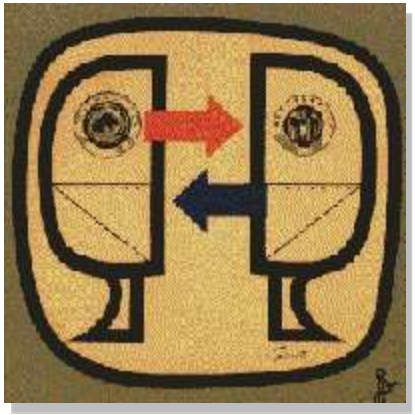
The Dynamics of Systems Changes

"There is no problem so complicated that you can't find a very simple answer to it if you look at it the right way."

-- Douglas Adams



Pink Floyd



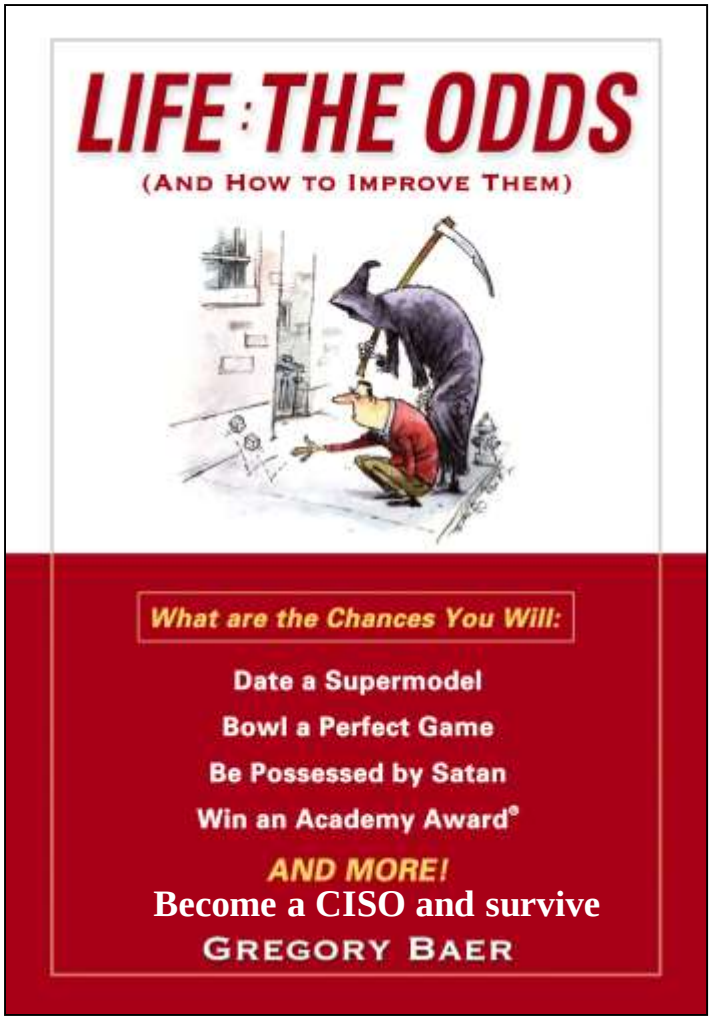
Norbert Wiener

The key to progress is the process of *feedback* in its most simple form, two-way communication.

Social Engineering … at its best…

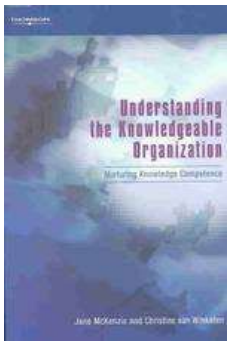
FoxTrot
by Bill Amend
WHAT ARE YOU DOING?
POSTING HOMEWORK ANSWERS ON THE INTERNET.
WHAT FOR?
UNLIKE HOLLYWOOD AND THE RECORDING INDUSTRY, I VIEW ONLINE COPYING AS A GOOD THING.
SOON, THROUGH THE MAGIC OF PEER-TO-PEER FILE SHARING, KIDS THE WORLD OVER WILL HAVE READY-TO-USE SOLUTIONS TO EVERY QUESTION IN MY TEXTBOOKS.' AND THERE'S NOT A THING TEACHERS CAN DO TO STOP IT.'
ISN'T IT GREAT?!
THIS IS SO UNLIKE YOU, JASON.
HOW SO?

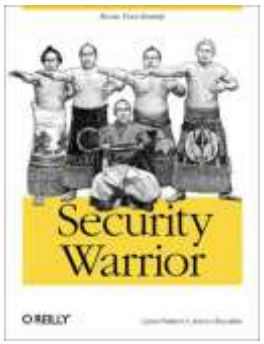
The future of information security is bright ..

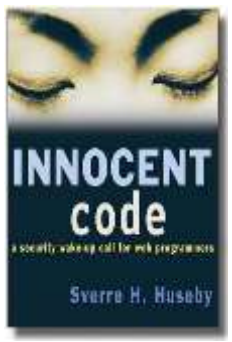


Colophon

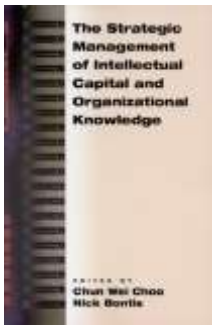
Managing the Unexpected

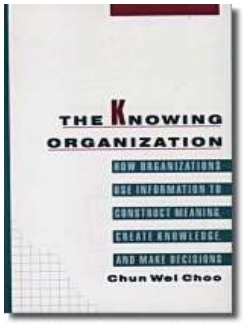

Understanding the Knowledgeable Organization

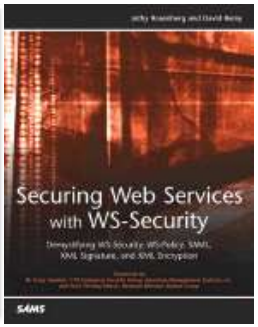

Security Warrior
O'REILLY


INNOCENT code
Sverre H. Huseby

THE SELF-ORGANIZING UNIVERSE
Erich Jantsch

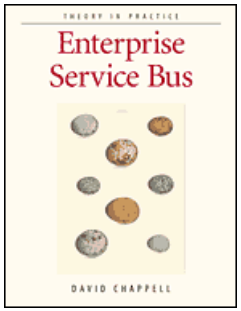

The Strategic Management of Intellectual Capital and Organizational Knowledge
Chun Wei Choo
Nick Bontis

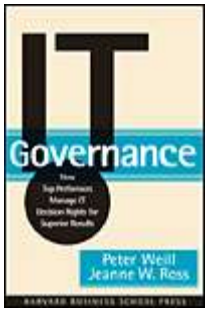

THE KNOWING ORGANIZATION
HOW ORGANIZATIONS USE INFORMATION TO CONSTRUCT MEANING CREATE KNOWLEDGE AND MAKE DECISIONS
Chun Wei Choo


Securing Web Services with WS-Security
SAMS

SPIROU et FANTASIO
LA MACHINE QUI RÊVE
TOME JANRY

INFO
Information
The New Language of Science
Hans Christian von Baeyer

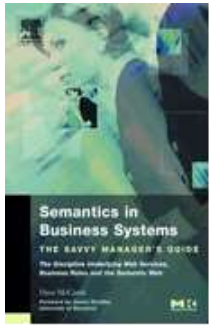

Enterprise Service Bus
DAVID CHAPPELL

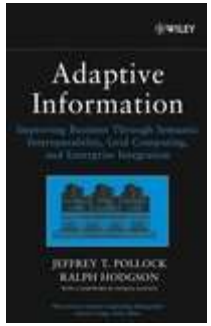

IT Governance
Peter Weill
Jeanne W. Ross

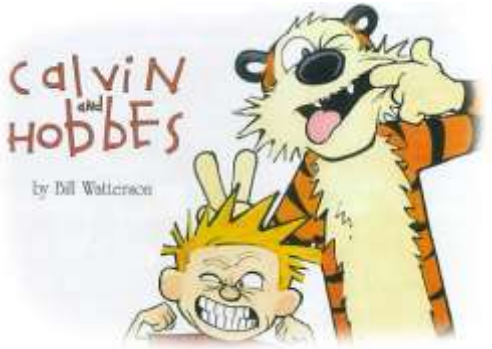
TRUST
FROM SOCRATES TO SPIN
KIERON O'HARA

the Ontology of Cyberspace

Ontological Engineering


Semantics in Business Systems
THE SAVVY MANAGER'S GUIDE


Adaptive Information
JEFFREY T. POLLOCK
RALPH HODGSON


calvin and hobbes
by Bill Watterson

Thank you